User Guide

hp StorageWorks IP Storage Router

SR2122-2

Product Version: 2.0

Third Edition (December 2003)

Part Number: 304835-003

This user guide provides instructional information for installing and configuring the HP StorageWorks IP Storage Router SR2122-2.

Printed in the U.S.A.

IP Storage Router SR2122-2 User Guide
Third Edition (December 2003)
Part Number: 304835-003

Contents

Figures

Tables

About This Guide

This user guide provides information to help you:

- Install the SR2122-2 IP Storage Router
- Configure the SR2122-2 IP Storage Router

“About this Guide” topics include:

Overview

This section covers the following topics:

Intended Audience

This book is intended for use by system administrators and technicians who are experienced with the following:

- Hardware installation and configuration.
- Ethernet and Fibre Channel Storage networks.

Prerequisites

Before you configure the storage router, make sure you review the following chapters and collect the information specified in Chapter 5.

- Chapter 4, Software Overview
- Chapter 5, Configuring the Storage Router

Related Documentation

In addition to this guide, HP provides corresponding information:

- *StorageWorks IP Storage Router 2122-2 Command Line Interface Reference Guide*
- *StorageWorks IP Storage Router 2122-2 Release Notes*

Conventions

Conventions consist of the following:

- Document Conventions
- Text Symbols
- Equipment Symbols

Document Conventions

The document conventions included in Table 1 apply in most cases.

Table 1: Document Conventions

Element	Convention
Cross-reference links	Blue text: Figure 1
Key and field names, menu items, buttons, and dialog box titles	**Bold**
File names, application names, and text emphasis	*Italics*
User input, command and directory names, and system responses (output and messages)	`Monospace font` `COMMAND NAMES` are uppercase monospace font unless they are case sensitive
Variables	`<monospace, italic font>`
Website addresses	Blue, underlined sans serif font text: http://www.hp.com

Text Symbols

The following symbols may be found in the text of this guide. They have the following meanings:

WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or death.

Caution: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

Note: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Equipment Symbols

The following equipment symbols may be found on hardware for which this guide pertains. They have the following meanings:

Any enclosed surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

WARNING: To reduce the risk of personal injury from electrical shock hazards, do not open this enclosure.

Any RJ-45 receptacle marked with these symbols indicates a network interface connection.

WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.

Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

WARNING: To reduce the risk of personal injury from a hot component, allow the surface to cool before touching.

Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

WARNING: To reduce the risk of personal injury from electrical shock, remove all power cords to completely disconnect power from the power supplies and systems.

Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manually handling material.

Rack Stability

Rack stability protects personnel and equipment.

WARNING: To reduce the risk of personal injury or damage to the equipment, be sure that:

- The leveling jacks are extended to the floor.
- The full weight of the rack rests on the leveling jacks.
- In single rack installations, the stabilizing feet are attached to the rack.
- In multiple rack installations, the racks are coupled.
- Only one rack component is extended at any time. A rack may become unstable if more than one rack component is extended for any reason.

Getting Help

If you still have a question after reading this guide, contact an HP authorized service provider or access our website: http://www.hp.com.

HP Technical Support

Telephone numbers for worldwide technical support are listed on the following HP website: http://www.hp.com/support/. From this website, select the country of origin.

Note: For continuous quality improvement, calls may be recorded or monitored.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP Storage Website

The HP website has the latest information on this product, as well as the latest drivers. Access storage at: http://www.hp.com/country/us/eng/prodserv/storage.html. From this website, select the appropriate product or solution.

HP Authorized Reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, see the HP website for locations and telephone numbers: http://www.hp.com.

Product Overview

1

This chapter is the starting point for installing the IP Storage Router 2122-2 hardware. It provides some very basic information you should know before proceeding to other chapters in this manual, and contains the following topics:

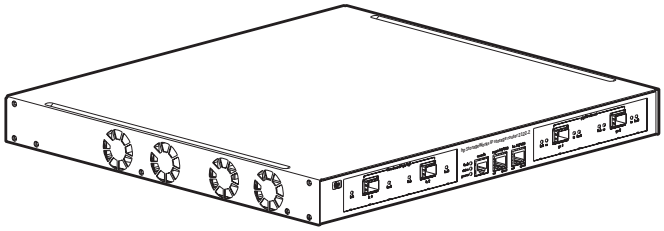
- Basic Description
- Port Descriptions
- Front-Panel LEDs
- Fan Assembly
- Power Supply

Installing and configuring a SR2122-2 storage router consists of the following tasks:

- Installing the storage router
- Configuring the storage router software
- Installing and configure the iSCSI drivers

Basic Description

The ST2122-2 is a 1U, rack-mountable storage router that provides IP hosts access to Fibre Channel storage through an IP network.



15001

Figure 1: Storage router chassis

The SR2122-2 provides access to Fibre Channel storage as if the IP hosts were directly attached to the storage. For more information about the types of storage access available with the storage router, see Chapter 4, "Software Overview" and other related documentation.

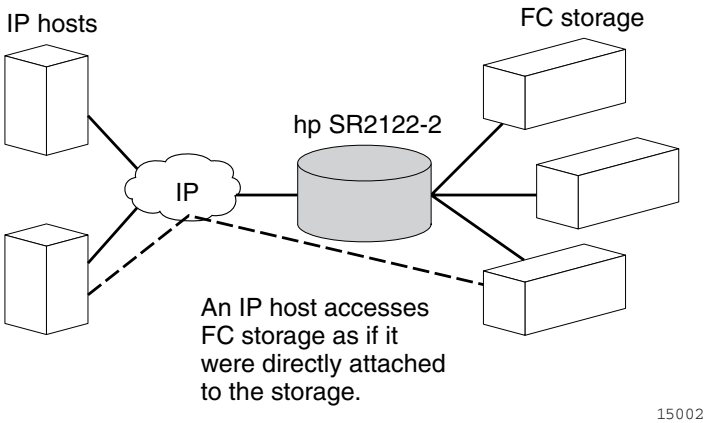
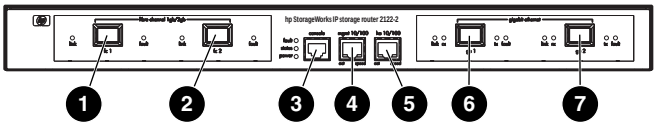


Figure 2: IP hosts accessing storage through the storage router

Port Descriptions

The SR2122-2 provides two 1-Gigabit Ethernet ports, a console port, a 10/100 Ethernet management port, a 10/100 Ethernet high availability (HA) port, and two 1-Gigabit/2-Gigabit Fibre Channel ports.



15003

Figure 3: Storage router ports

❶ Fibre Channel 1G/2G, FC 1
❷ Fibre Channel 1G/2G, FC 2
❸ Console port, CONSOLE
❹ 10/100 Ethernet management port, MGMT 10/100
❺ 10/100 Ethernet high availability (HA) port, HA 10/100
❻ Gigabit Ethernet, GE 1
❼ Gigabit Ethernet, GE 2

The following sections describe the ports:

- Gigabit Ethernet Ports
- Console Port
- 10/100 Ethernet Management Port
- 10/100 Ethernet HA Port
- Fibre Channel Ports

Gigabit Ethernet Ports

The Gigabit Ethernet ports are labeled GE 1 and GE 2 (see Figure 3). Each port provides a 1-Gigabit Ethernet interface for connecting to IP hosts that require access to storage. Each port uses a small form-factor pluggable (SFP) module for connection to the port's physical medium. See Appendix B, "Cable and Port Pinouts" for SFP module specifications. Each Gigabit Ethernet port has LEDs indicating its status, as described in Front-Panel LEDs, page 23.

Console Port

The console port is labeled CONSOLE (see Figure 3). It is an EIA/TIA-232 interface for connecting to the serial port of a PC running terminal emulation software. Using the console port, you can manage the storage router with the storage router command line interface (CLI). The console port uses an 8-pin RJ-45 receptacle; it has no LEDs.

Caution: The console cable may be connected to the unit during installation and maintenance only. The console cable must be disconnected from the unit when not in use during normal operation to minimize the electromagnetic interference.

10/100 Ethernet Management Port

The 10/100 Ethernet management port is labeled MGMT 10/100 (see Figure 3). It is a 10BaseT/100BaseT Ethernet interface for connecting to a management network. Through a management network, you can manage the storage router using the CLI, the web-based GUI, or SNMP. The 10/100 Ethernet management port uses an 8-pin RJ-45 receptacle and has LEDs indicating its status, as described in "Front-Panel LEDs" on page 23.

10/100 Ethernet HA Port

The 10/100 Ethernet high-availability (HA) port is labeled HA 10/100 (see Figure 3). It is a 10BaseT/100BaseT Ethernet interface for connecting to an HA network. The port allows the storage router to function in a multiple-node cluster with other storage routers to provide fault-tolerant operation. The 10/100 Ethernet HA port uses an 8-pin RJ-45 receptacle and has LEDs indicating its status, as described in "Front-Panel LEDs" on page 23.

Fibre Channel Ports

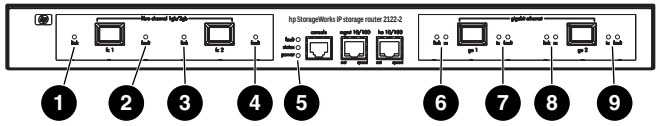
The Fibre Channel ports are labeled FC 1 and FC 2 (see Figure 3). Each port provides a 1-Gigabit/2-Gigabit Fibre Channel interface for connecting to storage systems, Fibre Channel switches, Fibre Channel hosts, or other HP storage networking products. Each Fibre Channel port can be configured as one of the following port types: G_Port, GL_Port, F_Port, FL_Port, or TL_Port. Each port uses a small form-factor pluggable (SFP) module for connection to the port's

physical medium. See Chapter B, “Cable and Port Pinouts” for SFP module specifications. Each Fibre Channel port has LEDs indicating its status, as described in the “Front Panel LEDs” section that follows.

Front-Panel LEDs

The front-panel LEDs provide status indications about the storage router chassis and its ports (see Figure 4).

- Each Gigabit Ethernet port, GE 1 and GE 2, has four LEDs, labeled LINK, RX, TX, and FAULT. The LEDs are located to the left and right of each Gigabit Ethernet port.
- The FAULT, STATUS, and POWER LEDs indicate the overall status of the storage router. The LEDs are located to the left of the CONSOLE port.
- The 10/100 Ethernet management port, MGMT 10/100, has two LEDs, labeled ACT and SPEED. The ACT LED is located at the left-bottom corner of the port; the SPEED LED is located at the right-bottom corner of the port.
- The 10/100 Ethernet HA port, HA 10/100, has two LEDs, labeled ACT and SPEED. The ACT LED is located at the left-bottom corner of the port; the SPEED LED is located at the right-bottom corner of the port.
- Each Fibre Channel port has two LEDs, labeled LINK and FAULT. The LEDs are located to the left and right of each Fibre Channel port.



15004

Figure 4: Front panel LEDs

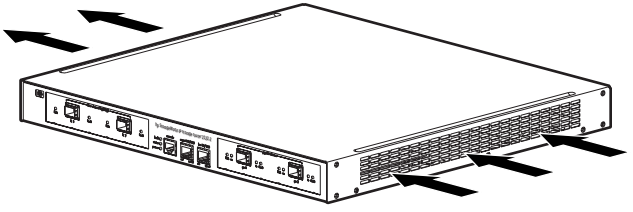
❶ FC 1 LINK
❷ FC 1 FAULT
❸ FC 2 LINK
❹ FC 2 FAULT
❺ FAULT, STATUS, POWER
❻ GE 1 LINK and RX
❼ GE 1 TX and FAULT
❽ GE 2 LINK AND RX
❾ GE 2 TX and FAULT

Table 2: Front panel LED descriptions

LED		Color	Description
GE 1 and GE 2 LEDs	LINK	Green	Port is operational
	TX	Green	Packets are being transmitted
	RX	Green	Packets are being received
FAULT		Red	On — Error in Storage Router
			Flashing — Error in a storage router component
Status		Green	On — Successful boot up
			Flashing — Booting up
POWER		Green	Power is on
MGMT 10/100 LEDs	ACT	Green	Link is active
	SPEED	Yellow	Port speed is 100 Mbps
HA 10/100 LEDs	ACT	Green	Link is active
	SPEED	Yellow	Port speed is 100 Mbps
FC 1 and FC 2 LEDs	ACT	Yellow	Frames are being transmitted or received
	LOG	Green	On — Port is properly connected
			Flashing once per second — Port is logging in
			Flashing twice per second — Port connection error

Fan Assembly

The fan assembly provides cooling for the internal chassis components. The storage router chassis contains four exhaust fans that are located on the left side of the chassis. The fans draw air in from the right and exhaust it out through the left.



15005

Figure 5: Chassis airflow

Power Supply

The SR2122-2 has an internal power supply that monitors its temperature and output voltages. The power supply automatically senses and adjusts to either of these input voltages: 115 VAC/60 Hz or 230 VAC/50 Hz.

If conditions reach critical thresholds, the power supply shuts down to avoid damage from excessive heat or electrical current. The power supply connects to site power through a power cord and the power connector on the rear panel. The power supply is powered on with a rocker switch next to the power connector. The switch is labeled I and O. Pressing I switches power on. Pressing O switches power off.

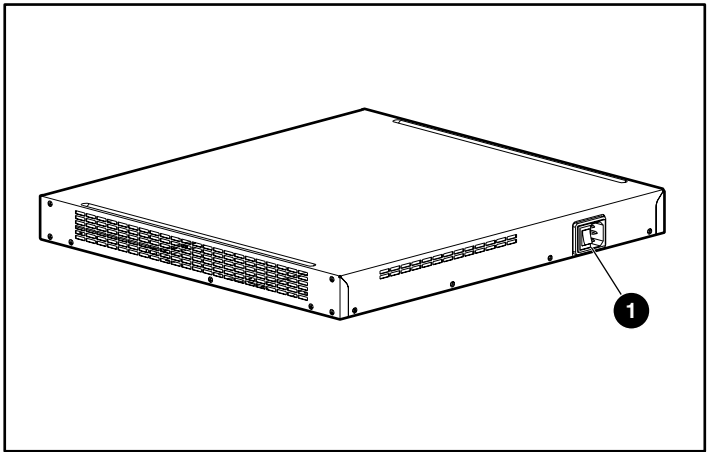


Figure 6: Rear panel, power connector

❶ Power Connector

Installation

2

This chapter describes how to:

- Prepare your site for installation
- Prepare and install the SR2122-2 storage router
- Connect network and Fibre Channel cables
- Connect power
- Verify correct installation

For first-time installations, perform the procedures in the following sections in the order listed here:

Site Planning

Planning the proper location and layout of your SR2122-2, your equipment rack, or wiring closet is essential for successful storage router operation. Equipment placed too close together or in a poorly ventilated area can cause the system to overheat. In addition, poor equipment placement can make system panels inaccessible and difficult to maintain.

Table 20 in Appendix A lists the operating and nonoperating environmental site requirements for the SR2122-2. Within specified environmental ranges, the system can continue to operate; however, a measurement that approaches the minimum or maximum of a range indicates a potential problem. You can maintain normal operation by anticipating and correcting environmental conditions before they exceed the maximum operating range.

Verify the site power for the type of device you are installing. Power requirements are useful for planning the power distribution system needed to support the storage router. Heat dissipation is an important consideration for sizing the air-conditioning requirements for an installation. See Table 20 in Appendix A for power and heat ratings for the SR2122-2.

Caution: To prevent a loss of input power, verify that the total maximum load on the circuit supplying power to the power supply is within the current ratings of the wiring and breakers.

Installing the Storage Router

You can install the SR2122-2 on a table or a shelf, or in an equipment rack. The following sections describe the steps required to install the storage router:

- Installing on a Table or a Shelf
- Rack-Mounting the Storage Router
- Installing SFP Modules

Installing on a Table or a Shelf

You can install the storage router on a table or a shelf (or another flat, secure surface).

If you are going to install the storage router in an equipment rack, skip this section and proceed to the "Rack-Mounting the Storage Router" section. To install the chassis on a table or a shelf:

1. Locate the four adhesive-backed rubber feet in the accessory kit that is shipped with the storage router.
2. Peel the rubber feet from their backing and place the feet onto the four round recessed areas on the bottom of the chassis.
3. Place the storage router on a table or a shelf near an AC power source.

Rack-Mounting the Storage Router

You can rack-mount the SR2122-2 in a 19-inch equipment rack with the front panel forward.

The accessory kit shipped with your storage router contains:

- two rails
- two wing nuts
- various screws

You need the following tools to install the SR2122-2 in a rack:

- Phillips screwdriver
- Tape measure

To install the SR2122-2 in a rack:

1. Prepare for installation:
    a. Place the storage router on the floor or on a sturdy table as close as possible to the rack. Leave enough clearance so that you can move around the storage router.
    b. Use a tape measure to measure the depth of the rack. Measure from the outside of the front mounting uprights to the outside of the rear mounting uprights. The depth must be at least 19 inches (48.26 cm) but not more than 32 inches (81.3 cm).

c. Measure the space between the inner edges of the left-front and right-front mounting uprights to ensure that the space is 17.75 inches (45.72 cm) wide.

2. Use the rack template provided to mark the center of a 1U mounting location on both sides of the front and rear mounting uprights.
3. Install cage nuts in the locations marked in step 2.

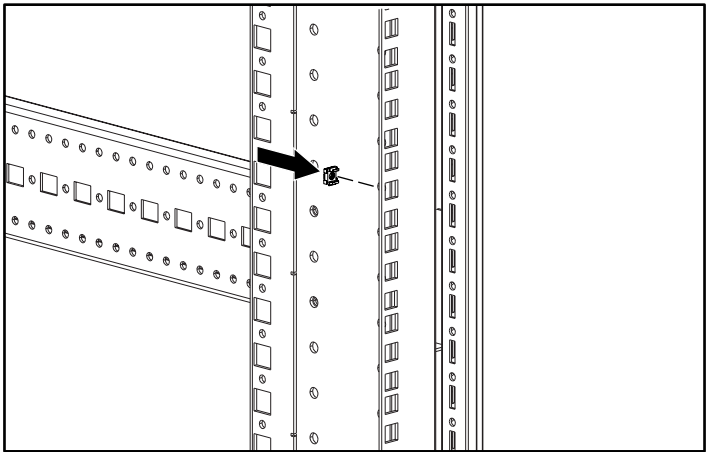


Figure 7: Installing cage nuts

4. Assemble the rails using the supplied wing nuts (see Figure 8).

Note: Do not tighten the wing nuts completely because the rails will need to be adjusted later in the installation process.

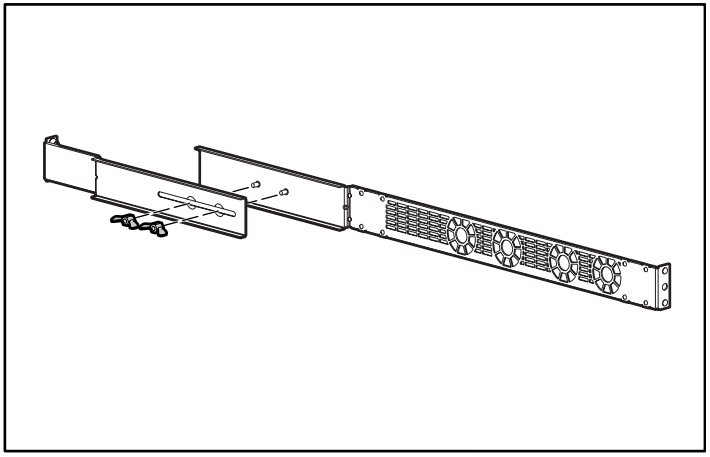


Figure 8: Rail assembly

5. Remove three existing screws from each side of the chassis (6 total).

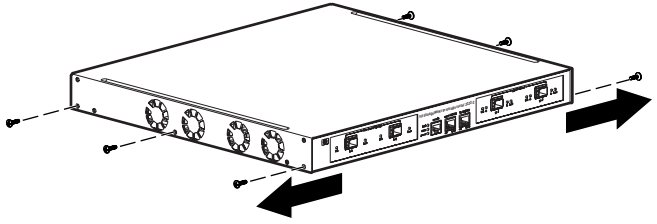


Figure 9: Removing the screws

6. Align and attach the rails to the chassis using the supplied flat-head screws.

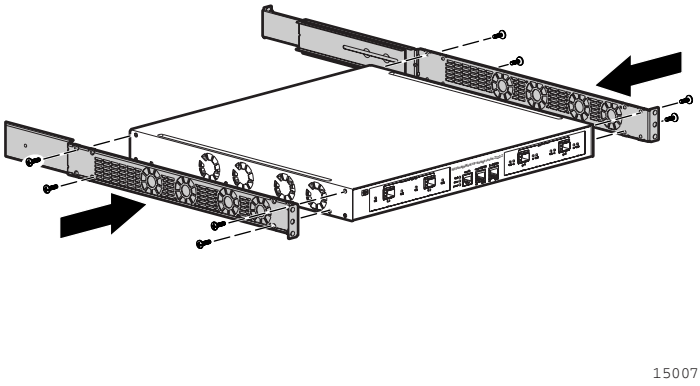


Figure 10: Attaching the rails

7. Slide the storage router into the rack and secure the front of the rails using the rack screws.

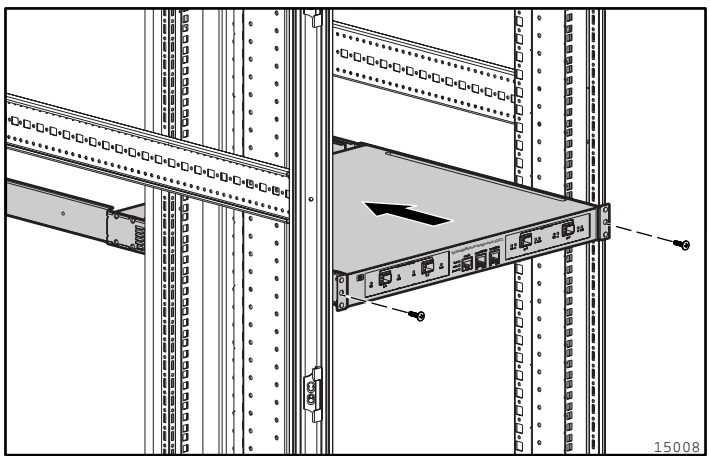


Figure 11: Installing the storage router into the rack

8. Adjust ❶ and secure the rear of the rails using the rack screws ❷ (see Figure 12).
9. Secure ❸ the rail halves by tightening the wing nuts.

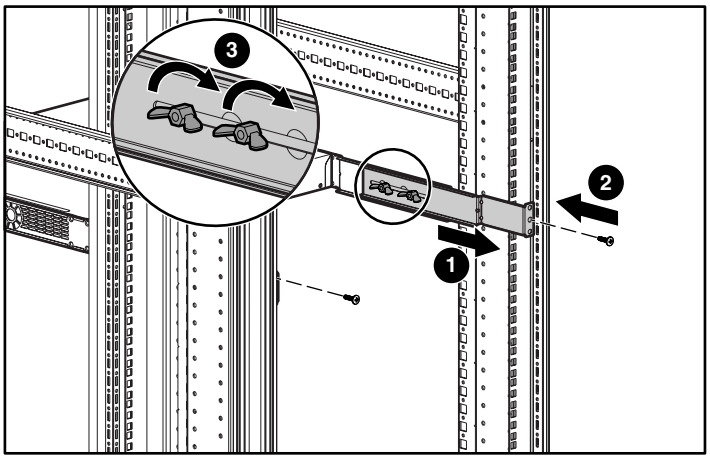


Figure 12: Securing the rear of the rails

Installing SFP Modules

Before installing or removing an SFP (small form-factor pluggable) module, read the installation information in this section. For connecting to SFP modules in the Gigabit Ethernet ports and the Fibre Channel ports, read the instructions in the "Connecting to Gigabit Ethernet and Fibre Channel Ports" section.

Note: Because of interoperability issues, HP does not support SFPs purchased from third-party vendors. See Chapter B, "Cable and Port Pinouts" for SFP port specifications.

Note: When fiber-optic cable plugs and SFP module receptacles are disconnected from each other, place dust covers on them.

WARNING: Because invisible radiation may be emitted from the aperture of the port when no fiber cable is connected, avoid exposure to radiation and do not stare into open apertures. To see translated versions of the warning, refer to the Regulatory Compliance and Safety document that accompanied the device.

The Gigabit Ethernet ports use fiber-optic SFP modules with either MT-RJ connectors (see Figure 13) or LC connectors (see Figure 14). The Fibre Channel ports use fiber-optic SFP modules with LC connectors (see Figure 14). Refer to Table 3 to determine what types of SFP modules you can install in the Gigabit Ethernet and Fibre Channel ports. See Appendix B, "Cable and Port Pinouts," for SFP module specifications.

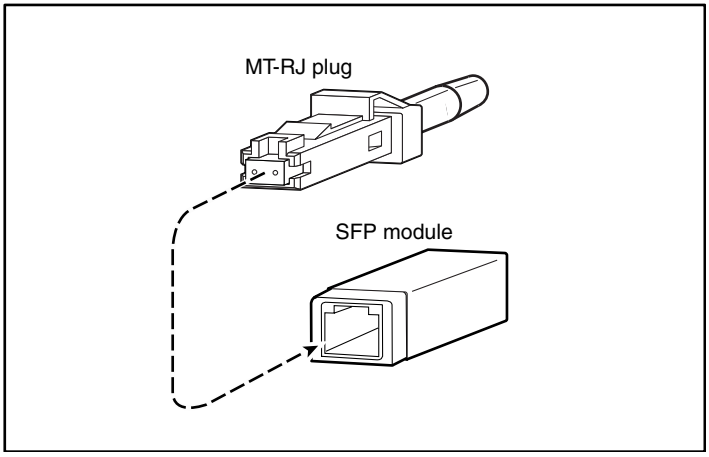


Figure 13: MT-RJ fiber-optic connector and SFP module

Caution: Protect your fiber-optic SFP modules by inserting clean dust covers into the SFPs after the cables are extracted from them. Be sure to clean the optic surfaces of the fiber cables before you plug them back into the optical bores of another SFP module. Avoid getting dust and other contaminants into the optical bores of your SFP modules; the optics will not work correctly when obstructed with dust.

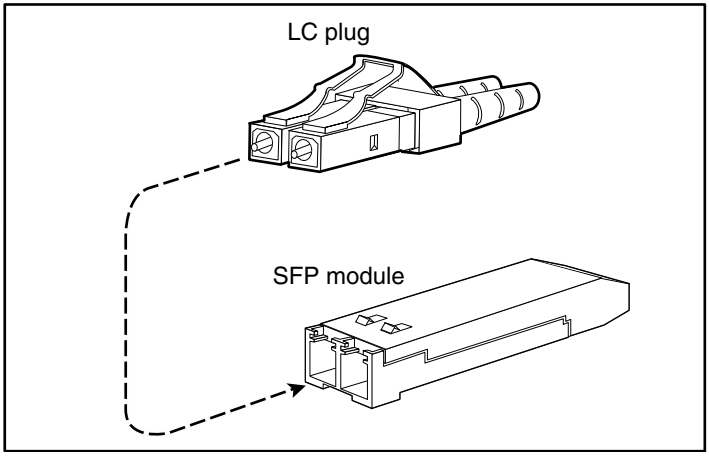


Figure 14: LC connector and fiber-optic SFP module

Table 3: Types of SFP Modules for Gigabit Ethernet and Fibre Channel ports

SFP Option Kit Part Number	Connector Type	Port
221470-B21	LC	Gigabit Ethernet or Fibre Channel

The SFP modules have three different types of latching devices used to secure and detach the SFP module from a port. The three types of SFP modules are described in the following sections:

- Mylar Tab SFP Modules
- Actuator/Button SFP Modules
- Bale Clasp SFP Modules

Mylar Tab SFP Modules

The Mylar tab SFP module has a tab that must be pulled to remove the module from a port.

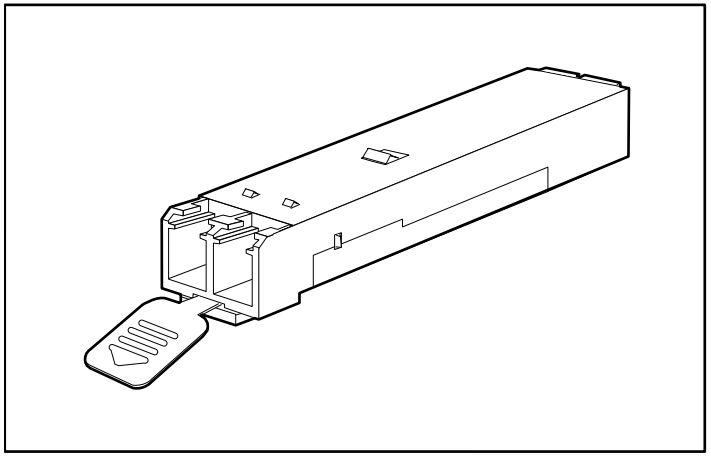


Figure 15: Mylar tab SFP module

To insert the Mylar tab SFP module into a port, line up the SFP module with the port, and slide it into place.

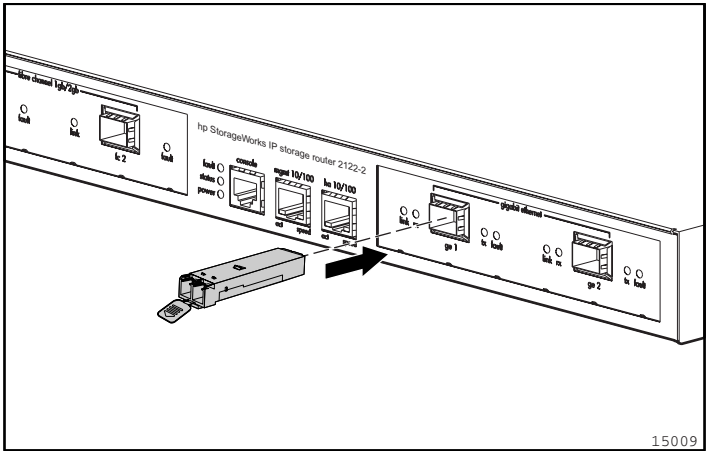


Figure 16: Inserting a Mylar tab SFP module

Caution: When pulling the tab to remove the SFP module, be sure to pull in a straight outward motion. Do not twist or pull the tab, you may disconnect it from the SFP module.

To remove the SFP module from the port, pull the tab gently in a downward direction until it disengages from the port, and then pull the SFP module out.

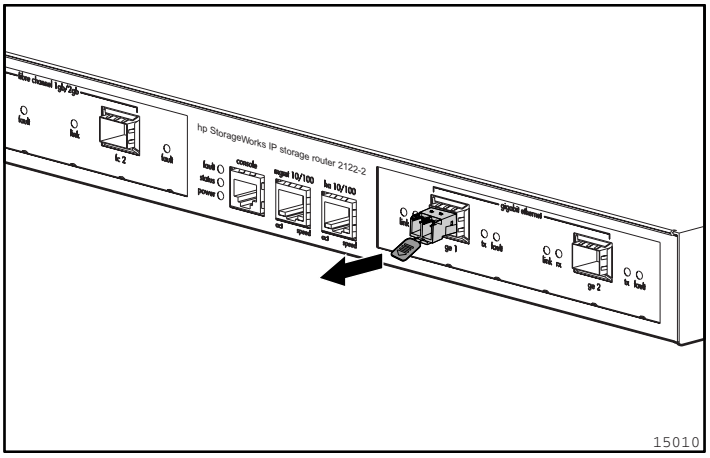


Figure 17: Removing a Mylar tab SFP module

Actuator/Button SFP Modules

The actuator/button SFP module has a button that must be pushed to remove the SFP module from a port.

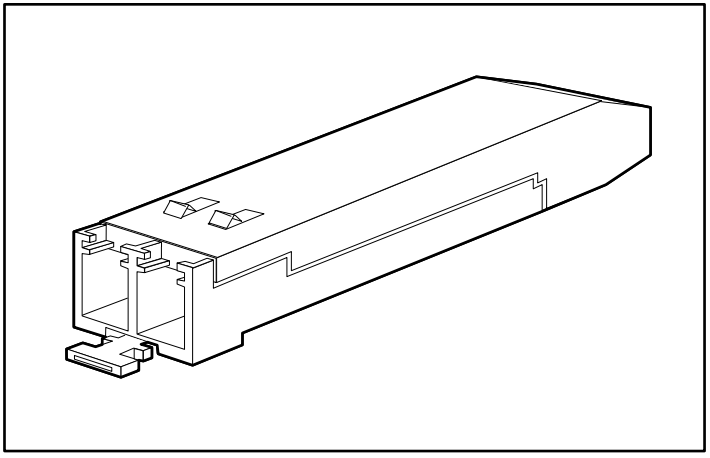


Figure 18: Actuator/button SFP module

To insert the actuator/button SFP module into a port, line up the SFP module with the port and slide it in until the actuator/button clicks into place. Be sure not to press the actuator/button as you insert the SFP module, you could inadvertently disengage the SFP module from the port.

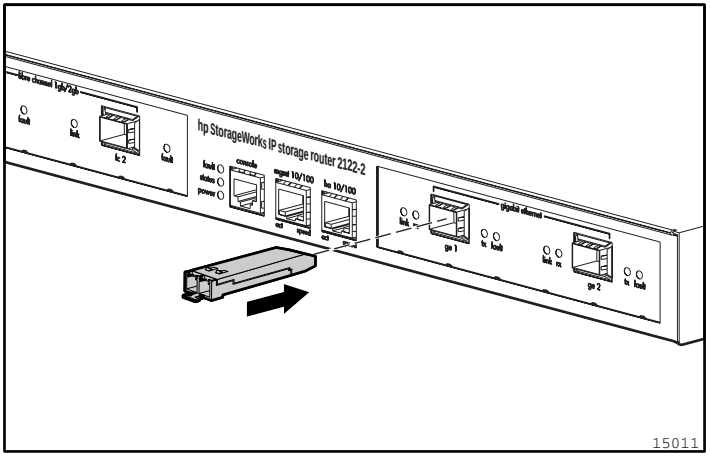


Figure 19: Inserting an actuator/button SFP module

To remove an actuator/button SFP module from a port:

1. Gently press the actuator/button ❶ on the front of the SFP module until it clicks and the latch mechanism releases the SFP module from the port.
2. Grasp the actuator/button between your thumb and index finger and carefully pull the SFP module ❷ from the port.

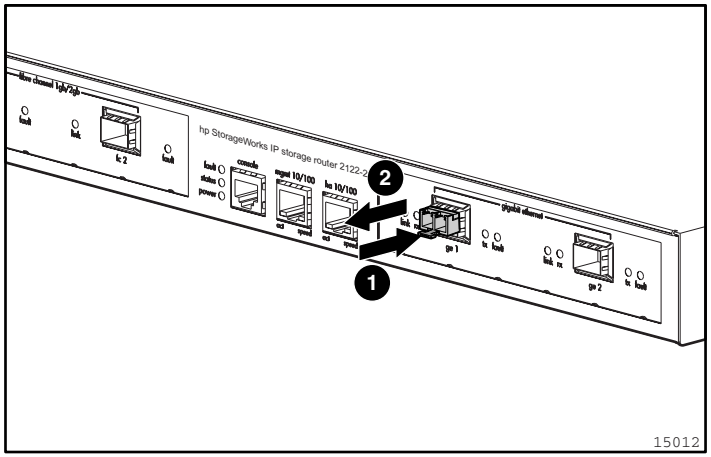


Figure 20: Removing an actuator/button SFP module from a port

Bale Clasp SFP Modules

The bale clasp SFP module has a bale clasp used to secure the SFP module in a port.

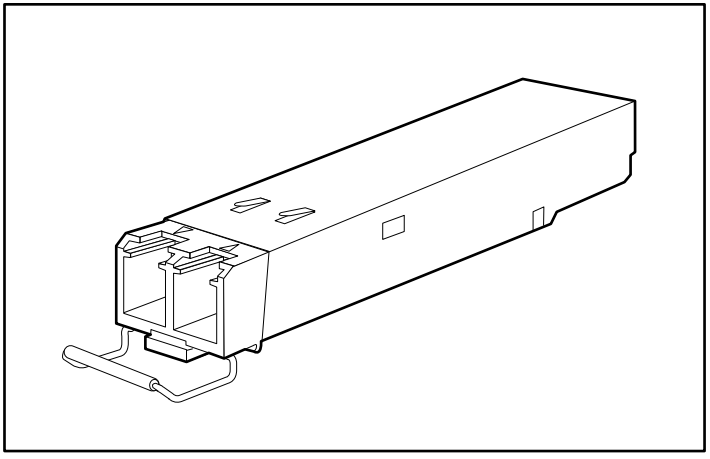


Figure 21: Bale clasp SFP module

To insert a bale clasp SFP module into a port:

1. Close the bale clasp before inserting the SFP module.
2. Line up the SFP module with the port and slide it into the port.

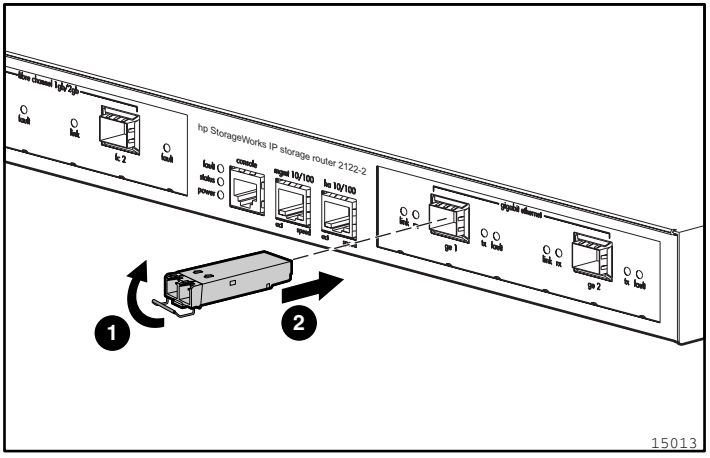


Figure 22: Inserting a bale clasp SFP module into a port

To remove a bale clasp SFP module from a port:

1. Open the bale clasp on the SFP module with your index finger, a small flat-blade screwdriver, or other long narrow instrument in a downward direction.

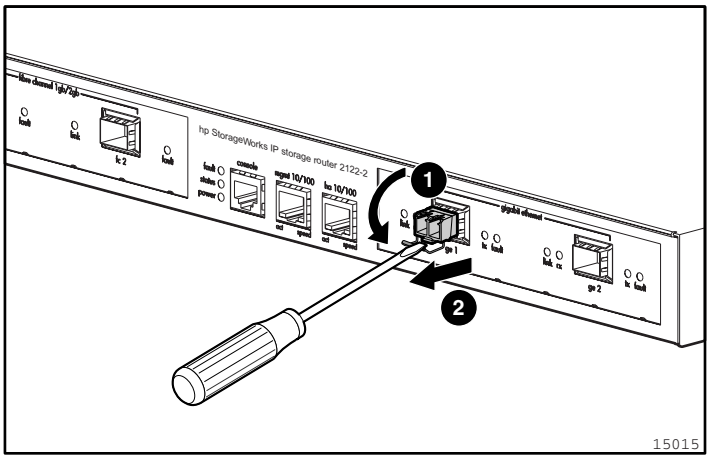


Figure 23: Removing a bale clasp SFP module with a flat-blade screwdriver

2. Grasp the SFP module between your thumb and index finger and carefully remove it from the port.

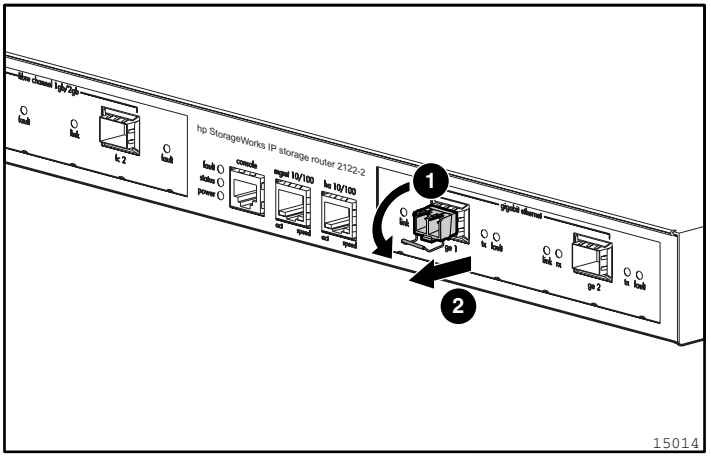


Figure 24: Removing a bale clasp SFP module from a port

Connecting to Gigabit Ethernet and Fibre Channel Ports

The Gigabit Ethernet ports, GE 1 and GE 2, use MT-RJ-type or LC-type fiber-optic SFP modules and cables. The Fibre Channel ports, FC 1 and FC 2, use LC-type fiber-optic SFP modules and cables. When connecting a cable to a fiber-optic SFP module, make sure that you firmly press the cable plug into the socket. The upper edge of the plug must snap into the upper front edge of the socket and you should hear the plug click when it is locked into the socket. To make sure that the plug is locked into the socket, gently pull on it.

To disconnect a plug from a socket, press the trigger on top of the plug, releasing the latch. You should hear a click, which indicates that the latch has released. Carefully pull the plug out of the socket.

Note: When you disconnect the fiber-optic cable from the module, grip the body of the connector. Do not grip the connector jacket-sleeve. Pulling on the sleeve can, over time, compromise the integrity of the fiber-optic cable termination in the connector.

Dirt or skin oils may have accumulated on an MT-RJ plug faceplate (around the optical-fiber openings), which can generate significant attenuation and reduce the optical power levels below threshold levels so that a link cannot be made. To clean an MT-RJ plug faceplate, follow this procedure:

1. Using a lint-free tissue soaked in 99 percent pure isopropyl alcohol, gently wipe the faceplate.
2. Remove any residual dust from the faceplate with compressed air before installing the cable.

Note: When fiber-optic cable plugs and SFP module receptacles are disconnected from each other, place dust covers on them.

The following sections describe how to connect cables to the Gigabit Ethernet and Fibre Channel ports:

- Connecting to a Gigabit Ethernet Port
- Connecting to a Fibre Channel Port

Connecting to a Gigabit Ethernet Port

To connect a cable to a Gigabit Ethernet port:

1. Remove the dust cover from the SFP module in the Gigabit Ethernet port; store the dust cover for future use.
2. Remove the dust cover (or covers) from the plug on the cable; store the cover (or covers) for future use. Insert the cable plug into the Gigabit Ethernet SFP module.
3. Connect the other end of the cable to the external end system, switch, or router.

Connecting to a Fibre Channel Port

To connect a cable to a Fibre Channel port:

1. Remove the dust cover from the SFP module in the Fibre Channel SFP port; store the dust cover for future use.
2. Remove the dust covers from the cable plug on the fiber-optic cable; store the dust covers for future use. Insert the cable plug into the Fibre Channel SFP module.
3. Connect the other end of the cable to a Fibre Channel port of another system (for example, a storage system, switch, host, or another storage router).

Connecting to the 10/100 Ethernet Management and HA Ports

To connect to the 10/100 management and HA ports:

1. Use modular, RJ-45, straight-through UTP cables to connect the 10/100 management and HA ports to end systems. Use modular, RJ-45 cross-connect cables to connect to external switches and routers.
2. Connect the appropriate modular cables to the 10/100 management and HA ports (see Figure 25).

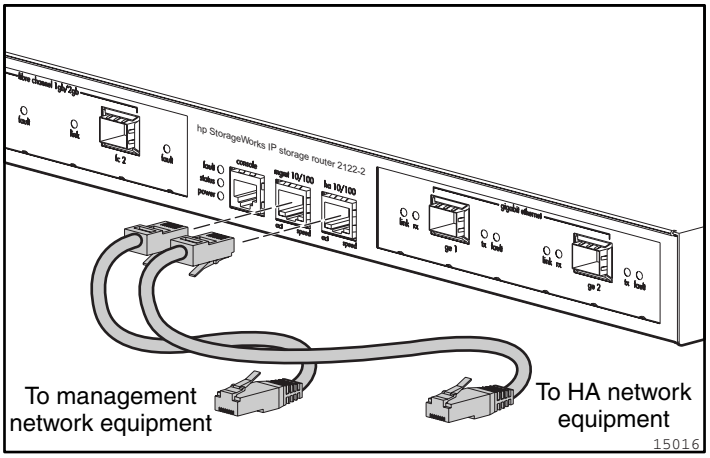


Figure 25: Connecting to the 10/100 management and HA ports

3. Connect the other end of the cable to the external end system, switch, or router.

Connecting to the Console Port

Connect a PC serial port to the console port for local administrative access to the storage router. The PC must support VT100 terminal emulation. The terminal-emulation software — frequently a PC application such as HyperTerminal or Procomm Plus — makes communication between the storage router and your PC possible during setup and configuration.

Caution: The console cable may be connected to the unit during installation and maintenance only. The console cable must be disconnected from the unit when not in use during normal operation to minimize the electromagnetic interference.

To connect to the console port:

1. Configure the PC terminal emulation program to match these console port default characteristics:

Table 4: Console port default characteristics

Console Port Default Characteristics	
Bits Per Second	9600
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

2. Connect the supplied RJ-45-to-DB-9 female adapter to the PC serial port.
3. Connect one end of the supplied console cable (a rollover RJ-45-to-RJ-45 cable) to the console port. Connect the other end to the RJ-45-to-DB-9 adapter at the PC serial port.

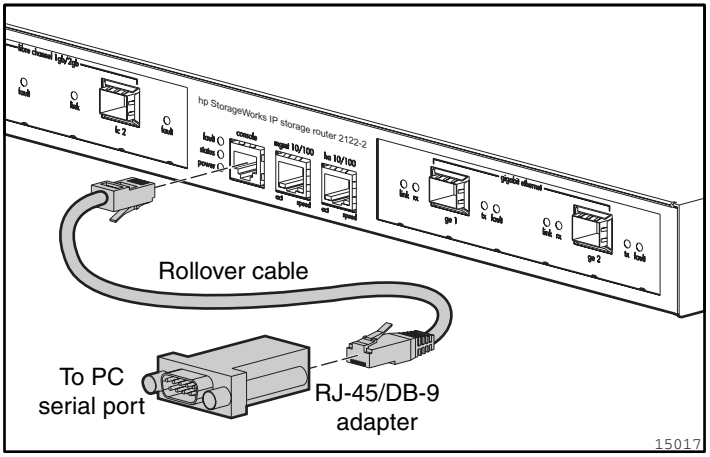


Figure 26: Connecting the console cable

Connecting Power

The SR2122-2 can be connected to either of two power sources: 115-120 VAC/60 Hz or 230-240 VAC/50 Hz. The power supply automatically senses the source and adjusts to either source.

To connect power to the storage router:

1. Make sure the power switch is set to Off.

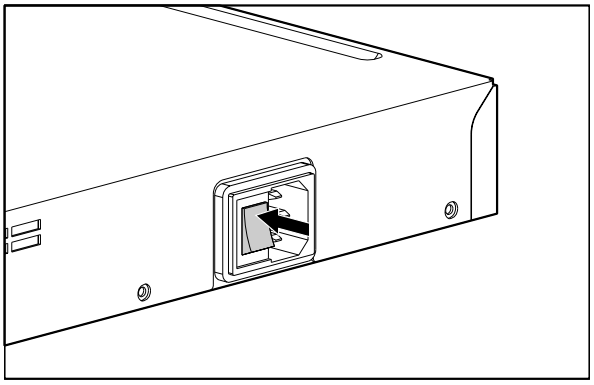


Figure 27: Power set to Off

2. Plug the power cord into the power receptacle located on the rear panel in the chassis.

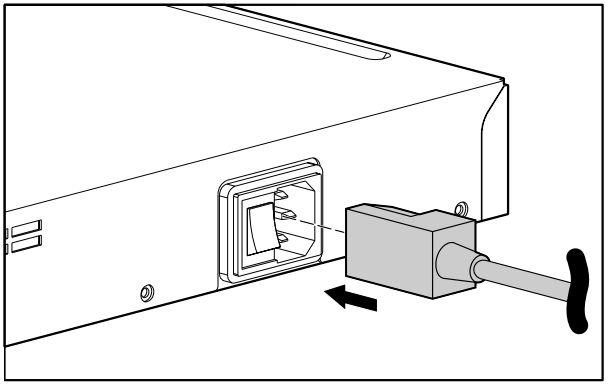


Figure 28: Connecting a power cord to the power connector

3. Connect the other end of the power cord to the power source for the storage router.

Verifying Installation

Verifying installation of the storage router consists of making sure that it starts properly and that the network and Fibre Channel connections are operational.

Verifying Startup Operations

To verify that the storage router starts up properly:

1. At the rear of the SR2122-2, press the power switch to the on position.
2. At the front of the SR2122-2, observe the POWER LED to make sure power is on. Make sure that the FAULT LED is off.
3. Listen and check for air flow to make sure the fan assembly is operating.
4. Observe console output to make sure that the storage router software is booting properly. The boot process may last for three to five minutes and will display boot information and a banner. A successful boot up is indicated by a CLI prompt for user input.
5. If any of these conditions are not met, refer to Chapter 3, “Troubleshooting” to isolate and, if possible, resolve the problem.

Verify that Network Connections are Operational

Verifying the network connections consists of making sure that the following ports are operational: Gigabit Ethernet, 10/100 Ethernet management, and 10/100 HA.

To verify that the network connections are operational:

1. Verify the Gigabit Ethernet port connections by checking the port link status LED. See Table 2 on page 24 for LED indication descriptions.
2. Verify the 10/100 Ethernet management port connection by checking the port link status LED. See Table 2 on page 24 for LED indication descriptions.
3. Verify the 10/100 HA port connection by checking the port link status LED. See Table 2 on page 24 for LED indication descriptions.
4. If any of these conditions are not met, see Chapter 3, “Troubleshooting” to isolate and resolve the problem if possible.

Verify That Fibre Channel Connections are Operational

To verify that the connections are operational:

1. Verify Fibre Channel port connections by checking Fibre Channel LOG LEDs. See Table 2 on page page 24 for LED indication descriptions.
2. If the LOG LEDs for connected ports are flashing, see Chapter 3, "Troubleshooting" to isolate and, if possible, resolve the problem.

Where to Go Next

Once you have verified that the storage router hardware is properly installed, it is ready for software configuration. To configure the software, refer to Chapter 4, "Software Overview"

Troubleshooting

3

This chapter provides troubleshooting procedures for problems encountered during installation of the SR2122-2 Storage Router and consists of the following sections:

Solving Problems at the Component Level

The key to troubleshooting the SR2122-2 is to isolate the problem on a specific storage router component. The first step is comparing what the storage router is doing to what it should be doing. Because a startup problem is usually attributed to a single component, it is more efficient to isolate the problem to a subsystem rather than troubleshoot each separate component in the storage router.

The SR2122-2 consists of the following subsystems:

- The power supply operates whenever system power is on (see "Troubleshooting the Power Supply" on page 52.
- The chassis fan assembly operates when the system power is on. The fan may continue to operate even when the power supply shuts down the storage router because of an over temperature or over voltage condition. The fan does not operate if the power switch is off.

  The following are simple checks you can make to determine if there is a fan problem:

  — Listen to the fan assembly to determine if it is operating.

  — Check for any obstructions restricting airflow through the storage router.

  If you determine that the fan assembly is not operating properly, contact a customer service representative.

Identifying Startup Problems

Observe the operation of the SR2122-2 and its front-panel LEDs to determine startup problems. LEDs indicate storage router status in the startup sequence. By checking the LEDs, you can determine when and where the storage router failed in the startup sequence.

To power up the storage router:

1. Listen for the chassis fan assembly operation. If it does not operate, see "Troubleshooting the Power Supply" on page 52. If you determine that the power supply is functioning normally and that the fan assembly is faulty, contact a customer service representative. If the fan assembly does not function properly at initial startup contact a customer service representative. There are no installation adjustments that you can make.
2. Check the POWER LED on the front panel. The POWER LED turns on immediately when power is on. The LED remains on during normal storage router operation. If the LED is not on, see "Troubleshooting the Power Supply" on page 52.
3. Check the STATUS and FAULT LEDs on the front panel. See "Front-Panel LEDs" on page 23 for LED descriptions.
4. Check the network and Fibre Channel port LEDs on the front panel. See the "Front-Panel LEDs" on page 23 for LED descriptions. If a network or Fibre Channel port LED indicates a problem with the port connection, see "Troubleshooting a Network or Fibre Channel Port Connection" on page 53.
5. Verify that the PC terminal emulation program is set correctly and that the PC is connected properly to the console port. Also, verify at the PC terminal emulation program display that the storage router has started up properly (for example, a prompt for starting a configuration wizard or a CLI prompt).
6. Contact a customer service representative for instructions if a status LED indicates a failure or if the PC connected to the console port indicates an incomplete boot-up process.

Troubleshooting the Power Supply

To help isolate a power problem:

1. Check the POWER LED.
   - If the POWER LED is off, verify that the power switch is in the on position.
   - If the power switch is on, unplug the power cord and then plug the power cord back in.
   - If the POWER LED remains off, continue with the next step.
2. Connect the power cord to another power source if one is available.
   - If the POWER LED comes on, the problem is the first power source.
   - If the POWER LED is off after you connect the power supply to a new power source, replace the power cord.
   - If the POWER LED still fails to light when the storage router is connected to a different power source with a new power cord, the power supply is probably faulty.
3. If you are unable to resolve the problem, contact a customer service representative for instructions.

Troubleshooting a Network or Fibre Channel Port Connection

If an LED on a network or Fibre Channel port indicates a problem, follow the steps in the next sections to isolate the problem:

- Troubleshooting a Connection to a Gigabit Ethernet Port
- Troubleshooting a Connection to a 10/100 Ethernet Management or 10/100 Ethernet HA Port
- Troubleshooting a Connection to a Fibre Channel Port

Troubleshooting a Connection to a Gigabit Ethernet Port

A bad connection to a Gigabit Ethernet (GE 1 or GE 2) port is indicated by the LINK LED being off. If the LINK LED is off:

1. Verify that the cable is connected properly and is in good operating condition.
   - Disconnect and connect both ends of the cable. If the LINK LED turns on, then the cable was not connected properly.
   - If the LINK LED remains off, replace the cable. If the LINK LED turns on, then the cable was defective.
   - If the LINK LED remains off, the cable is most likely not the problem. Continue to the next step.
2. Check the external end system, switch, or router to which the port is connected.
   - If the external end system, switch, or router is operating properly, continue to the next step.
   - If the external end system, switch, or router is not operating properly, then correct the problem. If the LINK LED turns on, then the problem was with the external end system, switch, or router.
   - If the LINK LED remains off, continue to the next step.
3. Replace the SFP module.
   - If the LINK LED turns on, the problem was the SFP module.
   - If the LINK LED remains off, contact a customer service representative for instructions.

Troubleshooting a Connection to a 10/100 Ethernet Management or 10/100 Ethernet HA Port

A bad connection to the 10/100 Ethernet Management or the 10/100 Ethernet HA port (MGMT 10/100 or HA 10/100) is indicated by the ACT LED being off. If the ACT LED is off:

1. Verify that the cable is connected properly and is in good operating condition.
   - Verify that the cable is the correct type of cable. (See Appendix B, “Cable and Port Pinouts.”)
   - Disconnect and connect both ends of the cable. If the ACT LED turns on, then the cable was not connected properly.
   - If the ACT LED remains off, replace the cable. If the ACT LED turns on, then the cable was defective.
   - If the ACT LED remains off, the cable is most likely not the problem. Continue to the next step.
2. Check the external end system, switch, or router to which the port is connected.
   - If the external end system, switch, or router is operating properly, continue to the next step.
   - If the external end system, switch, or router is not operating properly, then correct the problem. If the ACT LED turns on, then the problem was with the external end system, switch, or router.
   - If the ACT LED remains off, contact a customer service representative for instructions.

Troubleshooting a Connection to a Fibre Channel Port

A bad connection to a Fibre Channel port (FC 1 and FC 2) is indicated by the LOG LED flashing twice per second. If the LOG LED is flashing twice per second:

1. Make sure that the Domain ID of the Storage Router is configured properly. If the Domain ID is configured properly, continue to the next step.

Note: When a connection problem is resolved, the LOG LED will turn on after a brief logging-in period that is indicated by the LOG LED flashing once per second.

---

2. Verify that the cable is connected properly and is in good operating condition.
   - Disconnect and then re-connect both ends of the cable. If the LOG LED turns on, then the cable was not connected properly.
   - If the LOG LED remains off or flashing, replace the cable. If the LOG LED turns on (not flashing), then the cable was defective.
   - If the LOG LED remains off or flashing, the cable is most likely not the problem. Continue to the next step.
3. Check the device or switch to which the port is connected.
   - If the device or switch is operating properly, continue to the next step.
   - If the device or switch is not operating properly, then correct the problem. If the LOG LED turns on, then the problem was with the device or switch.
   - If the LOG LED remains off or flashing, continue to the next step.
4. Replace the SFP module.
   - If the LOG LED turns on, the problem was the SFP module.
   - If the LOG LED remains off or flashing, contact a customer service representative for instructions.

Contacting Customer Service

If you are unable to solve a startup problem after using the troubleshooting suggestions in this chapter, contact a customer service representative for assistance and further instructions. Before you call, have the following information ready to help your service representative assist you as quickly as possible:

- Date you received the SR2122-2
- Chassis serial number (located on the upper-right label on the rear panel of the chassis)
- Type of software and release number
- Maintenance agreement or warranty information
- Brief description of the problem
- Brief explanation of the steps you have taken to isolate and resolve the problem

See "Getting Help" on page 18 for information about how to contact HP Technical Support.

Software Overview

4

The IP Storage Router 2122-2 installation and configuration tasks consist of the following:

- Install the storage router according to Chapter 2, “Installation”
- Select how the storage router will be deployed: SCSI routing or FCIP.
- Configure the storage router software according to the guidelines in this guide.
- Install and configure iSCSI drivers in IP hosts connected to the storage router. The iSCSI driver is not required for FCIP deployment that have a TCP/IP Offload Engine (TOE) with embedded iSCSI protocol installed.

This chapter is the starting point for storage router software configuration. It provides some very basic, abbreviated information to help you understand storage router features and the software configuration process. It contains the following topics:

- Storage Router Overview
- SCSI Routing Overview
- FCIP Overview
- VLAN Access Overview
- Gigabit Ethernet Interface Overview
- Authentication Overview
- Cluster Management Overview
- Interface Naming

For guidance on choosing the correct configuration for your storage situation, please refer to Chapter E, “Recommended Host/Storage Configurations.”

Storage Router Overview

The storage router provides universal access to storage over IP networks. Storage router software controls the operation of the IP Storage Router 2122-2. The software is configured to provide the following types of access to storage over IP networks.

- SCSI routing only
- FCIP only
- SCSI routing and FCIP

SCSI routing provides IP hosts with access to Fibre Channel (FC) storage devices, using iSCSI protocol.

Note: The iSCSI protocol is an IETF-defined protocol for IP storage (ips). For more information about the iSCSI protocol, refer to the IETF standards for IP storage at http://www.ietf.org.

With SCSI routing, storage device access is managed primarily in the storage router.

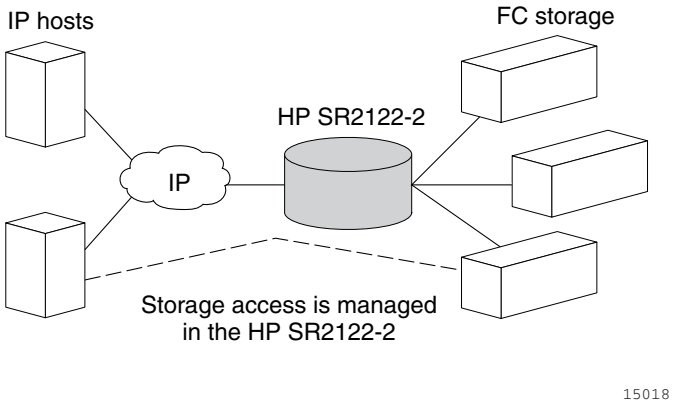


Figure 29: SCSI routing

Fibre Channel over IP (FCIP) enables SR2122-2 storage routers to provide connectivity by tunneling through an IP network between storage area networks (SANs).

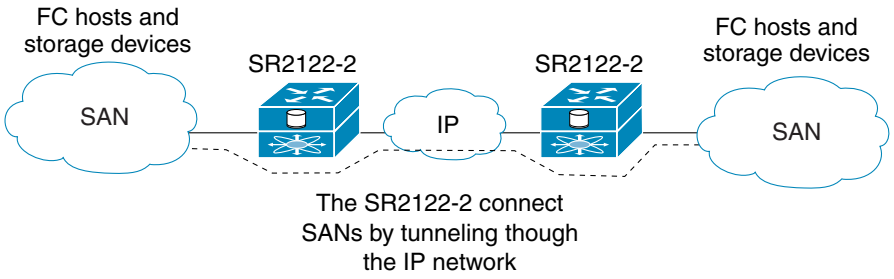


Figure 30: FCIP

In addition to providing services for accessing storage over IP networks, storage router software provides the following services:

- **VLAN Access Control** provides IP access control to storage based on a VLAN identifier (VID) number (in addition to access control through access lists).
- **Authentication** provides iSCSI authentication using AAA authentication methods.
- **High Availability (HA)** provides the ability to group storage routers in a cluster for failover and other cluster-related functions (for SCSI routing only).
- **E_Port with FC Fabric Zoning** provides the ability to connect FC ports to FC switches and participate in fabric zoning, manage zoning, and support zone mergers
- **SNMP/MIB support** provides network management of the storage router through SNMP using selected MIBs.
- **Gigabit Ethernet Interface features** provides the ability to assign a management IP address per Gigabit Ethernet interface, multiple IP addresses per SCSI routing instance, and an optional secondary Gigabit Ethernet interface per IP address used for SCSI routing or SR2122-2 management. When the SR2122-2 is deployed for FCIP, provides primary and optional secondary Gigabit Ethernet interfaces to the FCIP peer.
- **FCIP data compression** enables the SR2122-2 to dynamically compress FCIP data traffic for better channel bandwidth utilization.
- **Buffer credit extension** enables the SR2122-2 to donate buffer credits from a donor port to selected FC ports.

- **Secure Sockets Layer Support** provides HTTPS connection for secure access through the web-based GUI.
- **Secure Shell (SSH) protocol version 2 support** provides high encryption and authentication for interactive management sessions, and is a common replacement for Telnet.
- **Routing Information Protocol (RIP) listening support** allows the SR2122-2 to learn dynamic routing using RIP (version 1 or version 2) listening.
- **Service Location Protocol (SLP) support** provides the ability to advertise targets of specified SCSI routing instances to initiators or servers that use SLP.
- **Internet Storage Name Service (iSNS) support** provides the ability to register iSCSI targets with an iSNS server allowing iSCSI initiators to dynamically discover available storage targets.
- **LUN Trespass feature** provides a LUN failover feature for selected storage arrays that operate on the active/passive port model. When enabled, the trespass feature provides a redundant path from the storage router to the storage array by allowing the storage router to detect a path failure to a storage array port and perform the necessary operations to fail LUNs over to the other port on the storage array without using any multi-path software.
- **TCP Window Tuning** provides the ability to maximize bandwidth across the network by automatically setting the local TCP receive window size to the remote TCP receive window size without user intervention.
- **A command line interface (CLI) and a web-based GUI** provides user interfaces for configuration and maintenance of a storage router.

SCSI Routing Overview

SCSI routing provides IP hosts with access to FC storage devices as if the storage devices were directly attached to the hosts, with access to devices being managed primarily in the storage router. An iSCSI target (also called logical target) is an arbitrary name for a group of physical storage devices. The iSCSI targets are created and mapped to physical storage devices attached to the storage router. The SR2122-2 presents the iSCSI targets to IP hosts (iSCSI initiators) as if the physical storage devices were directly attached to the hosts. With SCSI routing, storage devices are not aware of each IP host; the storage devices are aware of the storage router and respond to it as if it were one FC host.

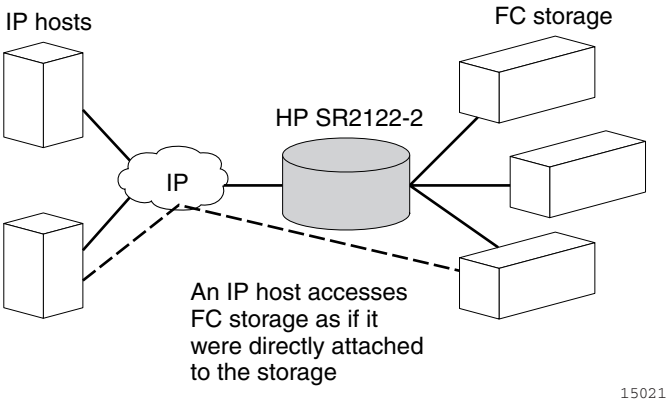


Figure 31: SCSI routing overview

To configure an IP Storage Router 2122-2 for SCSI routing, you should have a basic understanding of the following concepts:

- Routing SCSI Requests and Responses
- Basic Network Structure
- SCSI Routing Mapping and Access Control
- Available Instances of SCSI Routing

Note: Along with FC storage, FC host connections and FC switch connections are allowed; however, most of the illustrations in this manual show only storage connections for the purpose of describing the storage router features.

Routing SCSI Requests and Responses

SCSI routing consists of routing SCSI requests and responses between hosts in an IP network and FC storage.

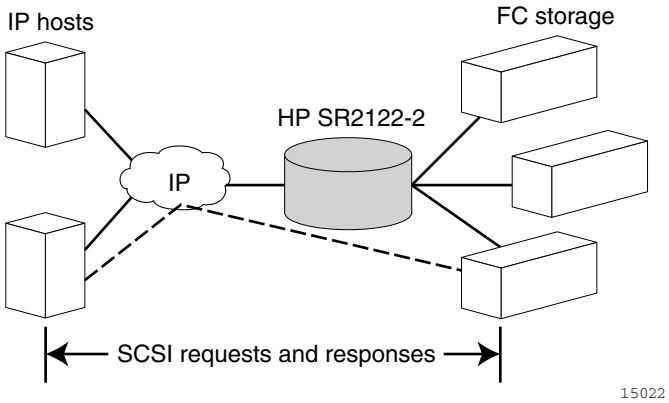


Figure 32: Routing SCSI requests and responses for SCSI routing

Each host that requires IP access to storage via an IP Storage Router 2122-2 needs to have a compatible iSCSI driver installed. Using the iSCSI protocol, the iSCSI driver allows an IP host to transport SCSI requests and responses over an IP network. From the perspective of a host operating system, the iSCSI drive appears to be a locally attached SCSI or Fibre Channel drive to the host.

SCSI routing consists of the following main actions (see Figure 33):

- Transporting SCSI requests and responses over an IP network between the hosts and the SR2122-2
- Routing SCSI requests and responses between hosts on an IP network and FC storage
- Transporting SCSI requests and responses between the SR2122-2 and FC storage

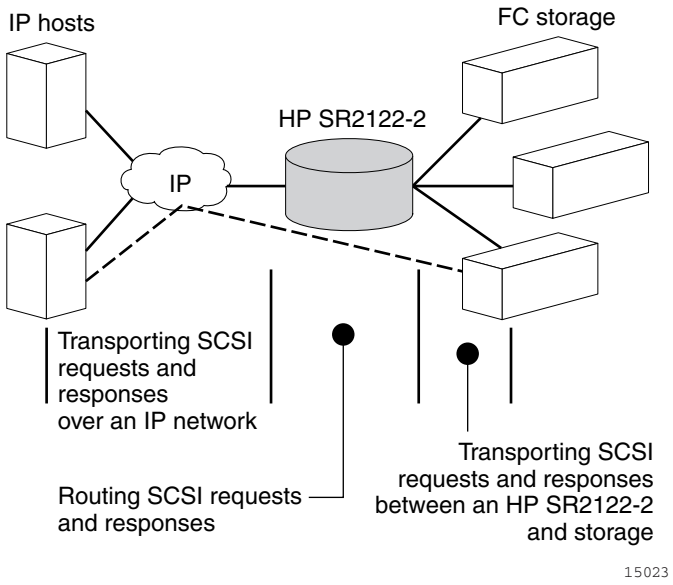


Figure 33: SCSI routing actions

Basic Network Structure

Figure 34 shows the basic structure of a SCSI routing network. IP hosts with iSCSI drivers access the storage routers through an IP network connected to the Gigabit Ethernet interface of each storage router. The storage routers access storage devices connected to the Fibre Channel interfaces of each storage router. A management station manages the storage routers through an IP network connected to the management interface of each storage router. For high availability (HA) operation, the storage routers communicate with each other over two networks: the HA network connected to the HA interface of each storage router and the management network connected to the management interface of each storage router.

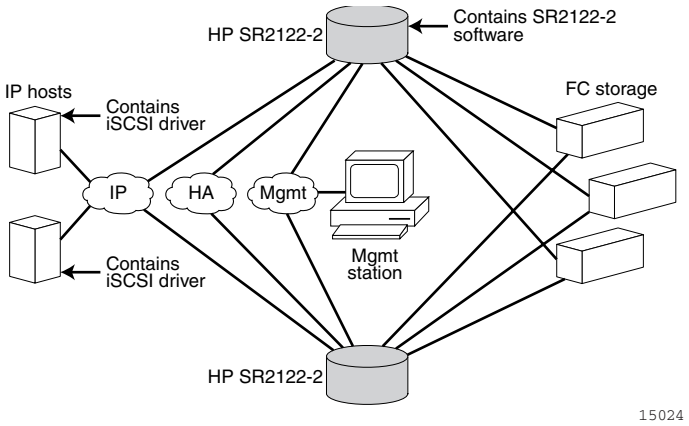


Figure 34: SCSI Routing basic network structure

SCSI Routing Mapping and Access Control

SCSI routing occurs in the storage router through the mapping of physical storage devices to iSCSI targets. An iSCSI target (also called logical target) is an arbitrary name for a group of physical storage devices. You can map an iSCSI target to multiple physical devices. An iSCSI target always contains at least one Logical Unit Number (LUN). Each LUN on an iSCSI target is mapped to a single LUN on a physical storage target.

You can choose either of two types of storage mapping: target-and-LUN mapping or target-only mapping. Target-and-LUN mapping maps an iSCSI target and LUN combination to a physical storage target and LUN combination. Target-only mapping maps an iSCSI target to a physical storage target and its LUNs.

With target-and-LUN mapping, an iSCSI target name and iSCSI LUN number are specified and mapped to the physical storage address of one LUN; either a WWPN + LUN (World Wide Port Name + LUN) combination, a LUN ID (unique LUN identifier), or a LUN serial number. If the LUN is available, it is made available as an iSCSI LUN and numbered with the iSCSI LUN number specified. For example, if an iSCSI target and iSCSI LUN specified as *Database*, *LUN 9* were mapped to the physical storage address, *WWPN 3100112233445566*, *LUN 12*, then *LUN 12* would be available as one iSCSI LUN. An iSCSI driver would see the iSCSI target named *Database*, with one iSCSI LUN identified as *LUN 9*. The iSCSI LUN would appear as one storage device to a host (see Table 5).

Table 5: Target and LUN Mapping Example

Apparent to Host	iSCSI Target	iSCSI LUN Available	Physical Storage Address	Physical LUN Available
Local Disk (D:)	Database	LUN 9	WWPN 31001122334 45566	LUN 12
Apparent as one locally attached storage device	Database appears as one controller with one LUN available	iSCSI LUN is numbered as specified and can be different than the physical LUN number	Specifies the storage address of the storage controller	The LUN number is specified as the only LUN to be mapped

With target-only mapping, an iSCSI target name is specified and mapped to the physical storage address of a storage controller only; a WWPN. Any LUNs that are available in the storage controller are made available as iSCSI LUNs and are numbered the same as the LUNs in the storage controller. For example, if an iSCSI target specified as *Webserver2000* were mapped to the physical storage address *WWPN 3100112233445577*, and *LUNs 0* through *2* were available in that controller, those LUNs would become available as three iSCSI LUNs. An iSCSI driver would see the iSCSI target named *Webserver2000* as a controller with three iSCSI LUNs identified as *LUN 0*, *LUN 1*, and *LUN 2*. Each iSCSI LUN would appear as a separate storage device to a host.

Table 6: Target-only Mapping Example

Apparent to Host	iSCSI Target	iSCSI LUN Available	Physical Storage Address	Physical LUN Available
Local Disk (D:)	Webserver2000	LUN 0	WWPN 3100112233445577	LUN 0
Local Disk (E:)	Webserver2000	LUN 1	WWPN 3100112233445577	LUN 1
Local Disk (F:)	Webserver2000	LUN 2	WWPN 3100112233445577	LUN 2
Apparent as three locally attached storage devices	Webserver2000 appears as one controller with one LUNs 0, 1, and 2 available	iSCSI LUNs are numbered the same as physical LUNs	Specifies the storage address of the storage controller	LUNs 0, 1, and 2 are available for mapping

Access for SCSI routing is controlled in the IP hosts and the storage router. In an IP host, the Gigabit Ethernet IP address of the SCSI routing instance in the storage router with which the host is to transport SCSI requests and responses is configured in the iSCSI driver. In a storage router, access is controlled through an access list and a VLAN identifier (VID) number of the hosts. Additionally, access can be further controlled in the storage router through authentication. See "Authentication Overview" on page 78 for more information about authentication.

An access list enables access to storage devices attached to the storage router with any combination of host IP address(es), CHAP user name(s), or iSCSI name(s). An access list contains these combinations. Host VID enables access to storage devices according to the VID of each host. See "VLAN Access Overview" on page 75 for more information about VLAN access.

For each iSCSI target you can associate one access list allowing read/write access, and one access list allowing read-only access. See Chapter 8, "Configuring SCSI Routing" for more information about read/write and read-only access.

You can use a combination of access lists and VIDs to configure access in the storage router; that is, you can specify that certain hosts according to IP address in a VLAN can access storage devices attached to the storage router.

Once the access is configured in the hosts and the storage router, and once the storage mapping is configured in the storage router, the storage router routes SCSI requests and responses between hosts and the mapped storage devices.

Figure 35 represents the concept of storage mapping and access control for SCSI routing. In the figure, the SR2122-2 provides three IP hosts with IP access to disk drives across four disk controllers. The storage router contains two SCSI routing instances: one configured with IP address 10.1.2.3 for the Gigabit Ethernet interface and the other with IP address 10.1.2.4. The iSCSI drivers in each IP host are configured to access those SCSI routing instances by their IP addresses through the Gigabit Ethernet interface. An access list in the storage router or VID (or both) specifies that hosts A, B, and C are allowed to access the mapped storage devices. From the perspective of a host, each disk drive mapped to it appears as a locally attached disk drive. Table 7 shows the correlation between an access list and/or VID, the Gigabit Ethernet IP addresses of the SCSI routing instances, and the storage device mapping.

Note: The purpose of Figure 35 and Table 7 is to illustrate the concept of storage mapping and access control. The IP addresses will vary according to each site. Similarly, the type of storage addressing (for example, LUNWWN, WWPN + LUN or LUN serial number) will vary according to the types of storage and the types of storage addressing preferred at each site. In addition, the figure and the table exclude any additional storage routers that could be configured for high availability.

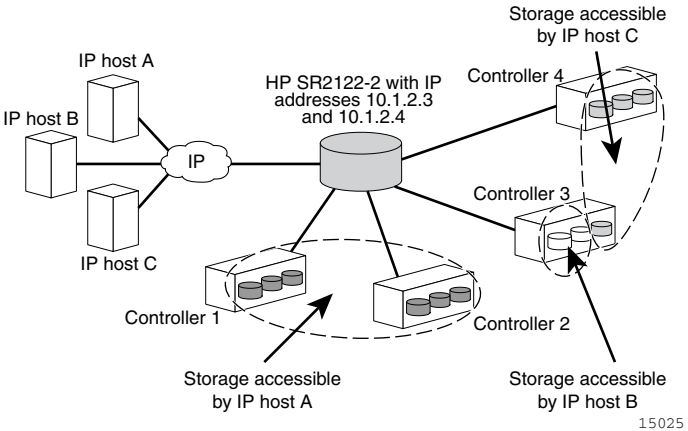


Figure 35: SCSI routing storage mapping and access control concept

Table 7: SCSI Routing Storage Mapping and Access Control Concept

Hosts allowed access via storage router access list and/or VID	Storage devices apparent to the host as locally attached devices	Via GbE IP addresses of SCSI Routing Instances	Mapped to controller	Mapped to drive
Host A	Local Disk (D:)	10.1.2.3	1	1
	Local Disk (E:)	10.1.2.3	1	2
	Local Disk (F:)	10.1.2.3	1	3
	Local Disk (G:)	10.1.2.3	2	1
	Local Disk (H:)	10.1.2.3	2	2
	Local Disk (I:)	10.1.2.3	2	3
Host B	Local Disk (D:)	10.1.2.3	3	1
	Local Disk (E:)	10.1.2.3	3	2
Host C	Local Disk (D:)	10.1.2.4	4	1
	Local Disk (E:)	10.1.2.4	4	2
	Local Disk (F:)	10.1.2.4	4	3
	Local Disk (G:)	10.1.2.4	3	3

Available Instances of SCSI Routing

You can configure an IP Storage Router with up to 12 SCSI routing services. Each service needs to be configured with a Gigabit Ethernet IP address, mapping between iSCSI target names and physical storage addresses, and access control.

When an SR2122-2 is part of a cluster, an instance of SCSI routing can run on only one storage router in a cluster at any given time. For more information about instances of SCSI routing in a cluster, see “Cluster Management Overview” on page 79. For more information about configuring a storage router, see the appropriate configuration chapters in this document.

FCIP Overview

Fibre Channel over IP (FCIP) enables SR2122-2 Storage Routers to provide connectivity between FC hosts and FC storage devices over an IP network.

To deploy FCIP, two SR2122-2 Storage Routers are required. Each system is configured for FCIP and connected to a SAN (or to any FC host or FC device). The peer systems are connected to each other through an IP network.

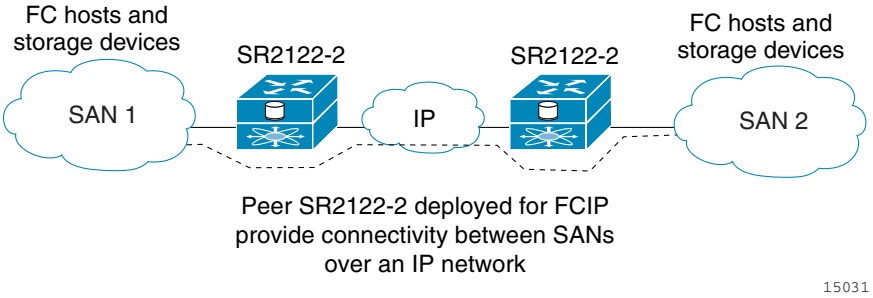


Figure 36: FCIP Overview

An FC host or FC device needs no additional hardware or software to access storage devices via an SR2122-2 Storage Router deployed for FCIP.

To configure an SR2122-2 Storage Router deployed for FCIP you need a basic understanding of the following concepts:

- Using FCIP to Route Fibre Channel Packets
- FCIP Network Structures

Using FCIP to Route Fibre Channel Packets

With FCIP, peer systems transport FC frames over an IP network. From the perspective of the SANs the storage devices accessed through the peer systems appear to be part of one unified SAN.

Once configured, FCIP instances on each system become active and establish their connectivity via the IP network. The storage devices in one SAN access the storage devices in the connected SAN using FC frames, which are encapsulated in IP packets by the FCIP instance, and transmitted to the peer system. The peer FCIP instance strips the IP packet data and passes only the FC frames over the FC interfaces to the storage devices.

The peer systems deployed for FCIP must be configured to use the TCP protocol. TCP protocol uses standard TCP flow control and error recovery algorithms and should be used if you require a standards-based FCIP implementation or connect to a non-SR2122-2 peer.

With the TCP protocol one FCIP instance must be configured as the TCP client; the other FCIP instance must be configured as the TCP server. The only difference between FCIP instances configured as TCP client and TCP server is which FCIP instance initiates the connection: the TCP client initiates the connection.

FCIP transports FC frames between SANs by performing the following actions (Figure 37):

- Transporting FC frames between a SAN and an SR2122-2 that is deployed for FCIP
- Encapsulating FC frames in IP packets and transporting the IP packets to a peer SR2122-2 that is deployed for FCIP
- Receiving IP packets and transporting as FC frames between the peer SR2122-2 and a connected SAN

Note that FC traffic is carried over the IP network in such a way that the FC fabric and all FC devices on the fabric are unaware of the presence of the IP Network.

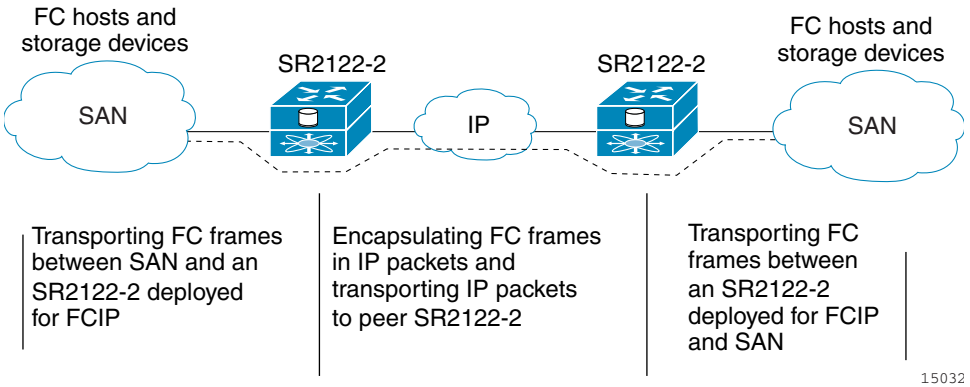


Figure 37: FCIP actions

FCIP Network Structures

This section describes typical FCIP network structures. In all of these examples a management station (not shown) manages the storage routers through an IP network connected to the management interface and/or HA interface of each storage router.

Figure 36 represents a basic, non-redundant structure of an FCIP network configuration. In this example an FC host or FC device connects to one or more Fibre Channel interfaces of each peer SR2122-2 Storage Router deployed for FCIP. Each SR2122-2 connects to the IP network through one of its Gigabit Ethernet interfaces. Through the IP network each FCIP instance accesses its peer, thereby connecting the SANs.

Figure 38 shows a slightly more complex FCIP network: a redundant WAN FCIP configuration. In this example configuration, an FC host or FC device connects to one or more Fibre Channel interfaces of each peer SR2122-2 Storage Router deployed for FCIP, and each SR2122-2 connects to two separate IP networks through each of its Gigabit Ethernet interfaces. Through the IP network, each FCIP instance accesses the peer storage router deployed for FCIP, connecting the SANs. In this configuration, IP A and IP B are redundant paths, so that the loss of connectivity via either path does not cause a loss of connectivity between the SANs.

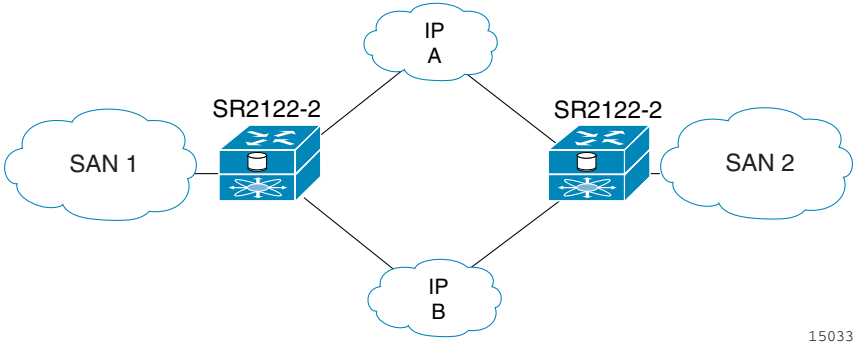


Figure 38: FCIP redundant WAN configuration

Figure 39 shows an even more reliable FCIP configuration, in which pairs of SR2122-2 Storage Routers provide full redundancy. In this configuration, loss of an SR2122-2 or loss of connectivity through one of the IP networks can be tolerated with no loss of connectivity between the SANs.

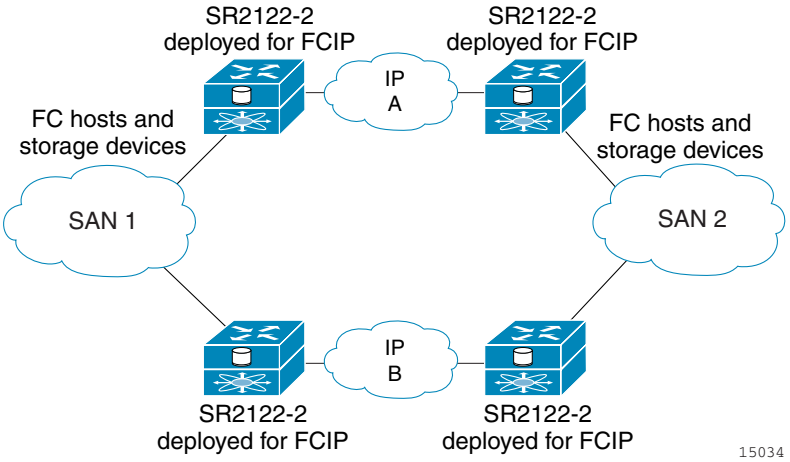


Figure 39: FCIP fully redundant configuration

Note: For multiple paths between SANs, multiple pairs of systems deployed for FCIP need to be connected to the FC hosts or FC devices. However, multiple SR2122-2 Storage Routers deployed for FCIP cannot be configured in an HA cluster. It is assumed that the multipath management is being done by an entity outside the SR2122-2 (for example, by management applications on the FC host or storage devices).

Figure 40 shows an alternative network structure for FCIP in which FCIP tunnels are established from two SANs aggregated to a central site. The SR2122-2 at the central site has one FCIP instance set up for SAN 1 and the other FCIP instance set up for SAN 2.

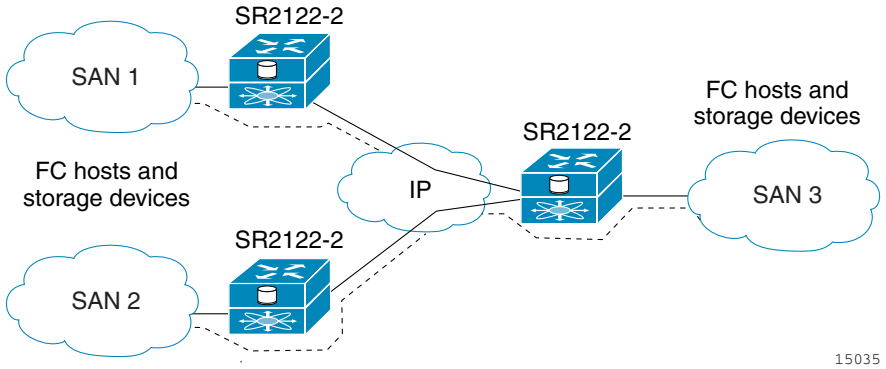


Figure 40: Multisite FCIP configuration

Mixed Mode Overview

When the SR2122-2 is deployed for SCSI routing you can optionally configure one of the internal FC initiator interfaces for FCIP. When it is deployed for FCIP, one of the internal FC initiator interfaces can be configured for SCSI routing. This mixed mode deployment allows the storage router to provide IP hosts with access to the FC storage via one initiator interface and FCIP connectivity for FC hosts and FC storage devices via the other initiator interface.

Figure 41 shows a storage router deployed for mixed mode, with one internal FC initiator interface dedicated to SCSI routing and the other internal interface dedicated to FCIP.

When the storage router is deployed for mixed mode, all of the features and functionality of the primary deployment mode (SCSI routing or FCIP), and the additional mode, are available.

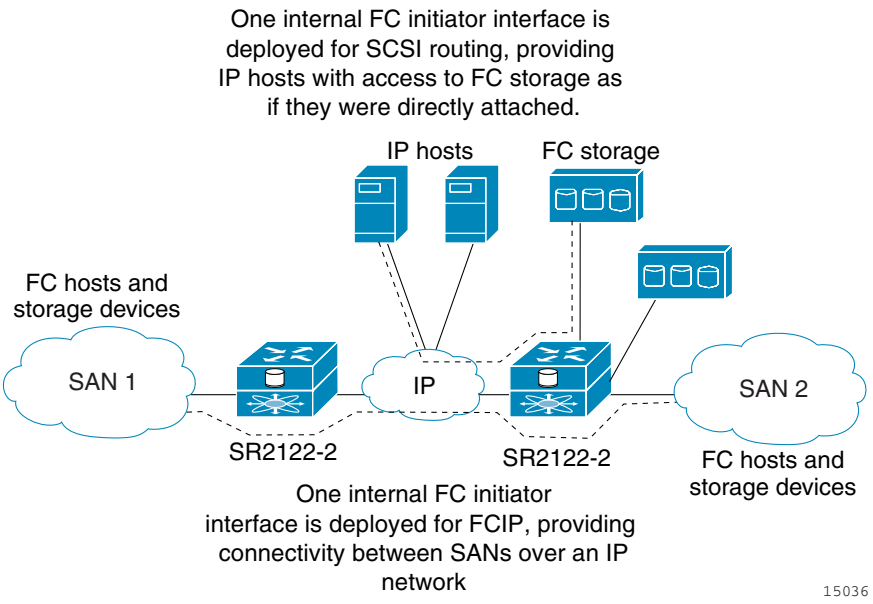


Figure 41: Mixed mode overview (SCSI routing and FCIP)

Basic Network Structure

When a storage router is deployed for SCSI routing and FCIP, IP hosts with iSCSI drivers access the storage router through the IP network connected to the storage router's Gigabit Ethernet interfaces. The storage router accesses the storage devices or intelligent storage array connected to the Fibre Channel interfaces. Access to the FC interfaces is made through the internal FC initiator interface configured for iSCSI traffic.

The internal FC initiator interface configured for FCIP allows the FC hosts or FC devices to connect to one or more Fibre Channel interfaces of the peer systems, which are connected to the IP network through a Gigabit Ethernet interface. Through the IP network, each FCIP instance accesses its peer, thereby connecting the SANs. Redundant network structures are also supported.

A management station manages the storage router through an IP network connected to the management interface. A storage router deployed for SCSI routing and FCIP can also participate in a cluster to provide HA operations for SCSI routing.

VLAN Access Overview

Storage router VLAN access provides IP hosts with access to storage devices according to the VLAN to which each host belongs.

Figure 42 shows a sample network that employs storage router VLAN access. In the figure, a storage router Gigabit Ethernet interface is connected to an IP network through an IEEE 802.1Q trunk; the storage router Fibre Channel interfaces are connected to storage devices 1, 2, and 3. The storage router is configured with two SCSI routing instances named *SR100* and *SR200*. The IP network contains two VLANs: VLAN 100 and VLAN 200. The SCSI routing instance, SR100, is configured to allow the hosts in VLAN 100 to access storage devices 1 and 2. The SCSI routing instance, SR200, is configured to allow the hosts in VLAN 200 to access storage device 3.

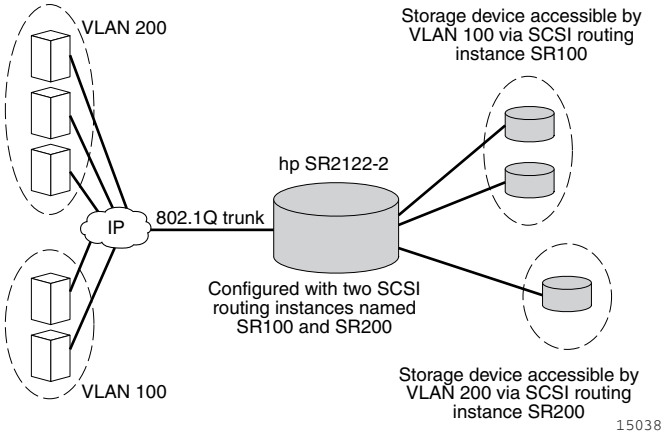


Figure 42: VLAN access overview

If the storage router is used in a switched network environment, configure the storage router using the proprietary VLAN Trunking Protocol (VTP). With VTP, the storage router will exchange VTP packets with an externally attached switch to dynamically learn about the VLANs that are accessible in the IP network. The storage router then uses VTP to propagate VLAN information around the switched network using layer 2 multicast packets.

If the storage router is used in a non-switched network environment, configure the storage router for VLAN without using VTP. The storage router does not exchange VTP packets to learn about the VLANs in the network. Instead, you must manually assign VLANs in the network with a VLAN identifier (VID) number. You can optionally assign each VLAN with a unique name and manually set the MTU size.

If the storage router participates in a cluster, the VLAN information configured for the storage router is propagated to all storage routers in the cluster.

The SR2122-2 uses IEEE 802.1Q standard for VLAN encapsulation. With 802.1Q encapsulation, VLAN information is carried in packets sent and received through the storage router Gigabit Ethernet interface. These packets contain the VID and other VLAN information needed for VLAN members to participate in a VLAN.

A VLAN is granted access to storage devices via a SCSI routing instance configured in the storage router. The iSCSI targets assigned to the SCSI routing instance determine which storage devices the VLAN can access.

Gigabit Ethernet Interface Overview

Each of the two 1-Gigabit Ethernet interfaces on the SR2122-2 (GE 1 and GE 2) provide the following capabilities:

- Multiple IP addresses per SCSI routing instance—allows IP hosts to connect to SCSI routing instances via one or more IP addresses. Each Gigabit Ethernet interface can be configured with up to 12 unique IP addresses which provides a maximum of 24 unique IP addresses per SR2122-2 Storage Router. If VLAN access is used, the maximum number of unique IP addresses per Gigabit Ethernet interface increases to 16. This provides a maximum of 32 unique IP addresses per SR2122-2 Storage Router when configured with VLAN.
- Assignment of a secondary interface per SCSI routing instance—allows the same IP address to be assigned to each Gigabit Ethernet interface; one interface is assigned as primary and one interface is assigned as secondary. If the primary Gigabit Ethernet interface loses connection to the host and if the secondary connection is assigned and still connected, the IP address moves to the secondary Gigabit Ethernet interface which then becomes active.
- Assignment as an interface to an FCIP peer—allows assignment of an IP address as a primary Gigabit Ethernet interface between an FCIP instance and an FCIP peer. Each SR2122-2 can be configured with up to two FCIP instances, and each FCIP instance can be configured with one peer for a maximum of two FCIP peers per SR2122-2 Storage Router when configured for FCIP.
- Assignment of a secondary interface per FCIP instance—allows the same IP address to be assigned to each Gigabit Ethernet interface configured for an FCIP instance; one interface is assigned as primary and one interface is assigned as secondary. If the primary interface loses connection to the network and remains down for two seconds, the IP address moves to the secondary Gigabit Ethernet interface, which then becomes active.
- Assignment as a management IP address—allows each Gigabit Ethernet interface to have one IP address assigned per logical interface, as a management interface. This IP address is in addition to any multiple IP address(es) per SCSI routing instance or FCIP instance assigned.
- Assignment of a secondary management IP address—allows the same IP address to be assigned to each Gigabit Ethernet interface configured as a management interface; one interface is assigned as primary and one interface is assigned as secondary. If connection to the primary Gigabit Ethernet

maintenance interface is lost and if the secondary maintenance interface connection is assigned and connected, the IP address moves to the secondary Gigabit Ethernet interface, which then allows management access.

Authentication Overview

Authentication is a software service that is available in each SR2122-2. It provides a method of identifying users (including login and password dialog, challenge and response, and messaging support) prior to receiving access to the requested object, function, or network service. The SR2122-2 supports three types of authentication:

- iSCSI authentication—provides an authentication mechanism to authenticate IP hosts that request access to storage. An IP host, acting as an iSCSI initiator, can also verify the identity of an iSCSI target assigned to a SCSI routing instance, which responds to the request, resulting in a two-way authentication.
- Enable authentication—provides a mechanism to authenticate users requesting Administrator mode access to an SR2122-2 management session via the CLI **enable** command or an FTP session.
- Login authentication—provides a mechanism to authenticate users requesting access to the SR2122-2 in Monitor mode via the login process from a Telnet session, SSH session or the SR2122-2 console.

Authentication is provided by an AAA (authentication, authorization, and accounting) subsystem configured in each SR2122-2. AAA is an architectural framework for configuring a set of three independent security functions in a consistent and modular manner: authentication, authorization, and accounting. The SR2122-2 Storage Router software implements the authentication function.

AAA authentication is configured by defining a list of authentication services. iSCSI authentication, which uses a AAA authentication services list, can be enabled for specific SCSI routing instances in an SR2122-2.

When iSCSI authentication is enabled, IP hosts (with iSCSI drivers) must provide user name and password information each time an iSCSI TCP connection is established. With two-way authentication, the SCSI routing instance to which an iSCSI target has been assigned responds to the authentication request with an assigned username and password. iSCSI authentication uses the iSCSI CHAP (Challenge Handshake Authentication Protocol) authentication method.

See Chapter 10, “Configuring Authentication” for more information about configuring authentication services.

Cluster Management Overview

You can configure storage routers in a cluster to allow the storage routers to back each other up in case of failure.

Note: A storage router can participate in a cluster only if it is deployed for SCSI routing.

A storage router cluster consists of two SR2122-2 storage routers connected as follows:

- Connected to the same hosts
- Connected to the same storage systems
- Connected to each other through their management and high availability (HA) interfaces

In a cluster, storage routers continually exchange HA information to propagate configuration data to each other and to detect failures in the cluster. The storage routers exchange HA information through two separate networks: one connected to the management interface of each storage router and the other connected to the HA interface of each storage router. To make sure that HA information is exchanged reliably between storage routers, the storage routers balance the transmission of HA information between the management and the HA interfaces.

A storage router cluster supports up to 12 active instances of SCSI routing. At any given time, an instance of SCSI routing can run on only one storage router in a cluster. The instance continues running on the storage router where it was started until one of the following actions occurs:

- The instance is explicitly stopped or failed over to the other storage router in the cluster.
- The instance automatically fails over to another storage router because an interface is unavailable or another software or hardware problem occurs.

See Chapter 11, “Configuring a High Availability Cluster” for more information about configuring a high availability cluster.

Interface Naming

Configuring the SR2122-2 Storage Router software requires that you understand hardware interface naming. This section describes the interface naming system used with the storage router hardware.

Each storage router interface is assigned a three-character name consisting of two lower case letters followed by a number. The letters designate the interface type; the number designates the chassis slot occupied by the interface.

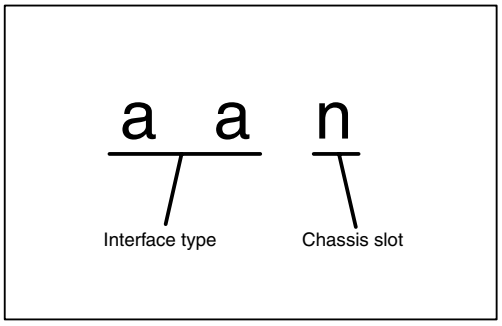


Figure 43: Storage router interface naming system

Table 8 shows valid interface type designators for the storage router; Figure 44 shows each interface location and interface name on the storage router.

Table 8: Interface Type Designators

Interface Type	Description
FC	Fibre Channel
GE	Gigabit Ethernet

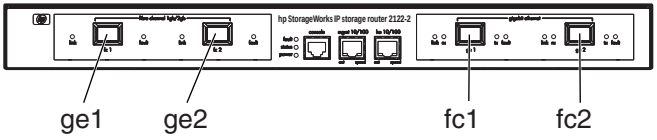


Figure 44: Storage router chassis-slot numbering

Configuring the Storage Router

5

This chapter describes the configuration information to gather and explains the initial system configuration script and setup configuration wizard for the first-time configuration of the IP Storage Router 2122-2. This chapter also introduces the command line interface (CLI) and web-based GUI, which can be used for subsequent configuration tasks.

This chapter contains the following sections:

Prerequisite Tasks

Before configuring the IP Storage Router 2122-2 for the first time, make sure you have completed the hardware installation according to the procedures in Chapter 2, "Installation."

Collecting Configuration Information

Use the storage router First-Time Configuration Checklist (see Table 10) to help you gather the system and network information is needed for the first-time configuration of your storage router. The items in the checklist are based on the information requested by the initial system configuration script and the setup configuration wizard. Refer to Table 9 for information on the configuration items needed for first-time configuration.

Table 9: Collecting Configuration Information

Configuration Item	Description	Required or Optional
Configuration deployment	SCSI routing (storage router enables iSCSI hosts to access Fibre Channel storage. Storage router manages access to the Fibre Channel storage.)	Required
Management interface IP address and subnet mask	The IP address and subnet mask of the storage router management interface. **Note:** The management interface for each storage router in a cluster must be on the same IP subnet.	Required
Static route for management interface	The destination IP address with subnet mask and then the gateway IP address.	Required if the storage router is managed from a subnet other than the one to which it is physically attached unless the SR2122-2 will be configured to use RIP listening (see Chapter 6, "Configuring System Parameters.")
System name	The name you want to use for the storage router. If you use the services of a domain name server (DNS), the system name is the same name you will enter and associate with the management interface. Maximum length is 19 characters.	Required
GE Interface	The Gigabit Ethernet interface used to communicate to the IP network, either ge1 or ge2. The default is ge1.	Required for SCSI routing only
High availability (HA) configuration	The storage router can run in either standalone or clustered mode. The default is clustered. Standalone mode is recommended if the storage router is not intended to provide high availability along with other storage routers.	Required for SCSI routing only

Configuration Item	Description	Required or Optional
High availability (HA) cluster name	The name of the cluster in which the storage router is to participate. Clusters are multiple storage routers that back each other up in case of hardware or software failure. All storage routers that participate in a cluster must have the same cluster name.	Required only if clustered was specified for the HA configuration
High availability (HA) IP address and subnet mask	The IP address and subnet mask of the storage router HA interface. The HA interface and management interface must be on unique IP networks. If the storage router is to participate in a cluster, the HA IP address is required; if the storage router is a standalone machine, it is optional. **Note:** The HA interface for each storage router in a cluster must be on the same IP subnet.	Required only if clustered was specified for the HA configuration
Primary DNS IP address	The IP address of the primary domain name server to be accessed by the storage router. Required if you refer to any other server via name rather than IP address.	Optional
Secondary DNS IP address	A backup domain name server from which the storage router can request services when the primary DNS is unavailable.	Optional
NTP server IP address	The IP address of the NTP server available to the storage router. This allows the storage router to keep the date and time synchronized with the rest of the network.	Optional
Time zone, current date and time	The format for the date is mm/dd/yyyy, and the time is hh:mm:ss.	Optional
Enable Telnet on all interfaces	Enable Telnet access on all interfaces. By default, Telnet access is enabled on only the management interface.	Optional
SNMP read community name	The name of the community having read-only access to the storage router network. The storage router will respond to this community's GET commands. The default is public.	Optional
SNMP write community name	The name of the community having write access to the storage router network. The storage router will respond to this community's SET commands. The default is private.	Optional
First SNMP trap manager IP address	The IP address of the first destination host used for SNMP notifications (traps). Required if you wish to use SNMP traps.	Optional
Trap version for first SNMP IP address	The version number of the traps that are to be sent to the first SNMP trap manager IP address. The default is 1.	Optional
Second SNMP trap manager IP address	An optional IP address of the second destination host used for SNMP notifications (traps).	Optional

Configuration Item	Description	Required or Optional
Trap version for second SNMP IP address	The version number of the traps that are to be sent to the second SNMP trap manager IP address. The default is 1.	Optional
Send authentication failure option	Enable an authentication failure trap to be sent when a user specifies an incorrect community.	Optional
Send link up/down traps option	Enable link up/down traps to be sent for the Management, HA, Gigabit, and/or Fibre Channel interfaces when the link goes up and when it goes down.	Optional
Monitor-level password	A password for users who will only monitor storage router operations. The default password is `hp`.	Optional
Administrator-level password	A password for users who will configure and administer the storage router. The default password is `hp`.	Optional
Password applied to EIA/TIA-232 console interface (yes/no)	Choose whether or not the user is required to enter the monitor and administrator password when accessing the storage router via the EIA/TIA-232 console interface. The default is `no`.	Optional
System administrator contact information	The name, e-mail address, phone number, and pager number of the system administrator of the storage router. Usage is completely site-specific.	Optional
Name of SCSI routing instance	A unique name for a SCSI routing instance. Names of instances can be up to 32 characters in length. A maximum of 12 unique SCSI routing instances are allowed. Only one instance can be named in the setup configuration wizard. **Note:** If the SR2122-2 is going to be a member of a cluster, do not define more than 12 SCSI routing instances across all storage routers in the cluster. For additional information about HA, cluster configuration and failover, see Chapter 11, "Configuring a High Availability Cluster." and Chapter 12, "Maintaining and Managing the Storage Router." **Note:** Do not name the SCSI routing instance with the setup configuration wizard if you are using the VLAN service with your storage router. See Chapter 7, "Configuring VLAN." before naming and configuring SCSI routing instances.	Required

Once you have completed the first-time configuration checklist, you are ready to continue with the first-time configuration of the storage router using the initial system configuration script and the setup configuration wizard.

Table 10: Storage Router First-Time Configuration Checklist

Configuration Item	Value
Configuration deployment option (1 or 2)	
Management interface IP address and subnet mask	
Static route for management interface	
System name	
GE Interface	
High availability (HA) configuration (standalone or clustered)	
HA cluster name	
HA interface IP address and subnet mask	
Primary DNS IP address	
Secondary DNS IP address	
NTP server IP address	
Enable Telnet on all interfaces (yes/no)	
SNMP read community name (default public)	
SNMP write community name (default private)	
First SNMP trap manager IP address	
Trap version for first SNMP IP address	
Second SNMP trap manager IP address	
Trap version for second SNMP IP address	
Send authentication failure trap when incorrect community specified (yes/no)	
Modify link up/down traps for one or more interfaces (yes/no)	
Send link up/down traps for Management interface (yes/no)	
Send link up/down traps for HA interface (yes/no)	
Send link up/down traps for Gigabit Ethernet interface (yes/no)	
Send link up/down traps for Fibre Channel interface (yes/no)	
Monitor-level password	
Administrator-level password	

Configuration Item	Value
Apply passwords to EIA/TIA-232 console interface (yes/no)	
System administrator name	
System administrator e-mail address	
System administrator phone number	
System administrator pager number	
Name of SCSI routing instance (if using the VLAN service, do not configure a SCSI routing instance with the setup configuration wizard)	
Configuration deployment option (1 or 2)	
Management interface IP address and subnet mask	

Connecting a Console

To begin configuration of your IP Storage Router 2122-2, use the command line interface (CLI), by connecting a PC with a terminal emulation program to the EIA/TIA-232 console interface according to the procedures in Chapter 2, "Installation." Then make sure that the terminal emulation program is configured for a CLI session with the values provided in Table 11.

Table 11: Terminal Emulation Configuration

Setting	Value
Data bits	8
Bit per second	9600
Parity	None
Stop bits	1
Flow control	None

Initial System Configuration Script

The initial system configuration script runs on the CLI and ensures that a few required values are entered to make the SR2122-2 operational. When you first power up the storage router and after the initial boot process, the script will run automatically on the CLI session running on the terminal emulation program via an EIA/TIA-232 console connection.

After the first running of the script, the script will run automatically whenever the storage router is not configured with an IP address for the management interface, due most likely to a `clear conf` command, which requires you to reconfigure the system.

The initial system configuration script provides explanatory text before prompting you to enter configuration values. The values asked for by the script are determined by the configuration deployment option entered for the first prompt.

Table 12 lists the configuration items in the order they will appear in the script.

Table 12: Configuration items in Initial System Configuration Script

Configuration Item	Configuration Deployment
Configuration deployment option: 1 for SCSI routing, 3 for FCIP	All
Management interface IP address and subnet mask in CIDR style (for example: 10.1.10.244/24)	All
The destination IP address with subnet mask and then the gateway IP address (for example: 1.0.1.0/24 10.0.1.2) (Optional)	All
IP Storage Router system name (maximum length allowed is 19 characters)	All
HA configuration (standalone or clustered)	SCSI routing
Cluster name (asked for only when HA configuration is set to clustered)	SCSI routing
HA interface IP address and subnet mask in CIDR style (for example: 10.1.20.56/24; asked for only when HA configuration is set to clustered)	SCSI routing
Mixed mode selection: reserve an internal FC port for FCIP	SCSI routing

When the script completes, the system automatically reboots. When the command prompt returns, continue configuration with the setup configuration wizard.

Running the Setup Configuration Wizard

The Setup Configuration Wizard is available from the CLI and is a script consisting of a series of prompts asking you to enter values to provide a basic system configuration for your storage router. You will be asked to enter values to configure the following:

- Management interface — includes primary and secondary DNS servers
- Date and time — includes time zone and NTP server
- Network management access — includes SNMP
- Management access — includes passwords and system administrator contact information
- System administrator contact information
- SCSI routing — this section of the wizard only appears if SCSI routing was the configuration deployment selected in the initial system configuration script; if you are using the VLAN service, do not configure SCSI routing with the Setup Configuration Wizard
- FCIP — this section of the wizard only appears if FCIP was the configuration deployment selected in the initial system configuration script

You can run the Setup Configuration Wizard through an EIA/TIA-232 console interface connection, or through a Telnet session using the management interface if the IP address is already configured in the storage router. If you choose to complete the configuration using the management interface, use the default password, `hp`, to establish your CLI session.

The values entered for the Setup Configuration Wizard are saved at the end of the wizard script. To quit the configuration wizard at any time without saving changes, press **Ctrl-C**, and reboot the storage router to restore previous values.

Note: The factory default listening port used for iSCSI traffic is 3260. This is a port number assigned by IANA. You can change this value for your network configuration if needed. See the *HP StorageWorks IP Storage Router 2122-2 Command Line Interface Reference Guide* for details.

Use the following procedure to start the Setup Configuration Wizard:

1. `enable` — Enter Administrator mode. If prompted for an Administrator password, use the default password, `hp`.

Note: Passwords are cluster-wide configuration elements and apply to all storage routers in a cluster. If the SR2122-2 joined an existing cluster during initial configuration, enter the Administrator mode password already configured for the cluster.

---

2. `setup` — Start the setup configuration wizard. The wizard will ask you to choose one of the two levels:
   - The novice level provides information before the prompt explaining what is being requested.
   - The expert level does not provide the explanatory text.

   Respond to the prompts using your First-Time Configuration Checklist.
   - For multiple choice questions, the choices are shown in square brackets
   - For values requiring a specific format, the required format is shown in square brackets.
   - If values have already been entered (for instance, via the initial system configuration script), the current values saved in the system are shown in square brackets.
   - Default values are shown in parentheses within the square brackets.
   - If you want to accept the current or default value, press **Enter**.
   - If there is no default and you want to bypass the question (that is, you do not want to change or provide a value), press **Enter**.

If you configured any interfaces or identified any servers to the IP Storage Router that are outside the storage router management subnet, you must update the storage router route table with the appropriate gateways that will provide access to these interfaces or servers (use the `ip route` command), or configure the SR2122-2 for RIP listening to dynamically learn IP routes. See Chapter 6, "Configuring System Parameters." for details on adding the static routes or configuring the SR2122-2 for RIP listening.

You can use the `setup` command again to change these basic configuration parameters. You can also use the command line interface (CLI) or the web-based GUI to make changes to the basic storage router configuration or to configure the SR2122-2 more extensively. To access the web-based GUI, point your browser to the storage router management interface IP address.

Introducing the CLI

The CLI is available via a Telnet session to the management interface. It is also available via a direct EIA/TIA-232 connection on the console interface. The CLI provides commands to perform all necessary storage router management functions, including software upgrades and maintenance.

All CLI commands are capable of prompting for further information as the user types.

- Pressing the Tab key completes the current command word at any point after it is unique.
- Pressing the question mark (`?`) key lists all of the options available at that point in the command syntax.
- Each command or keyword can be truncated at any point after it is unique.

For complete information on all storage router commands, see the *HP StorageWorks IP Storage Router 2122-2 Command Line Interface Reference Guide*.

Character Case Sensitivity in the CLI

CLI commands, keywords, and reserved words are not case-sensitive. Commands, keywords, and reserved words can be entered in upper and lower case. User-defined text strings can be defined in both upper and lower case (including mixed cases) and is preserved in the configuration.

Command Modes

The storage router management interface is password protected. You must enter passwords when accessing the storage router via Telnet (for the CLI) or web-based GUI.

There are two levels of authority:

- **Monitor mode** allows view-only access to the storage router status and system configuration information.

- **Administrator mode** allows the user to configure and actively manage the storage router, its access lists and SCSI routing instances, and the storage router cluster.

Passwords for Monitor and Administrator mode can be initially configured through the Setup Configuration Wizard (see "Running the Setup Configuration Wizard" on page 89). The factory default password for both modes is `hp`.

Note: Passwords are shared cluster-wide and when configured on the first storage router in the cluster, will be shared with any other storage router that joins the cluster.

Command Prompt

The CLI command prompt includes the storage router system name. An asterisk (`*`) appears at the beginning of the prompt if the system configuration has been modified but not saved.

Reserved Words

Reserved words cannot be used as values or names in CLI commands. Words that are used as commands or as keywords in commands are reserved words. The following are additional reserved words in the CLI.

- `acl`
- `canonical`
- `iprouter`
- `iptan`
- `loglevel`

Show CLI Command

Use the `show cli` command to display the complete CLI command syntax tree, along with helpful information about command parameters and arguments. Only valid commands will display for the current command mode of your IP Storage Router.

You can choose specific commands to display by specifying desired commands with the `show cli` command. For example,
`show cli aaa debug scsirouter` displays the syntax tree for all aaa commands, all debug commands, and all scsirouter commands.

Special Keys

The CLI supports the use of special keyboard keys. Table 13 lists the special keys and describes their function.

Table 13: Special Keys

Key	Function
`?`	List choices
`Backspace`	Delete character backwards
`Tab`	Command word completion
`Ctrl-A`	Go to the beginning of the line
`Ctrl-B or Left Arrow`	Go backwards one character
`Ctrl-D`	Delete current character
`Ctrl-E`	Go to the end of the line
`Ctrl-F or Right Arrow`	Go forward one character
`Ctrl-K`	Delete from current position to the end of the line
`Ctrl-N or Down Arrow`	Go to the next line in the history buffer
`Ctrl-P or Up Arrow`	Go to the previous line in the history buffer
`Ctrl-T`	Transpose the current and previous character
`Ctrl-U`	Delete the line
`Ctrl-W`	Delete the previous word

Starting a CLI Management Session

Follow these steps to start a CLI management session via a Telnet connection to the storage router.

1. Establish a Telnet session to the storage router.
2. Enter the appropriate password at the logon prompt.
3. Enter `enable` to change to Administrator mode. (Optional)

Note: If you need to make changes to the configuration of the storage router, you need to enable the Administrator mode.

---

4. Enter the Administrator password at the prompt. (Optional)
5. Issue the appropriate CLI commands to complete the desired task.

Introducing the Web-Based GUI

As an alternative to the CLI, you can configure your storage router using the web-based GUI. You can use the GUI for configuration after completing the initial system configuration script, which assures that the storage router management interface is configured with an IP address.

To access the GUI, enter the URL for the storage router by pointing your browser to the storage router management interface IP address using the HTTP protocol (for example, type `http://10.1.10.244`).

Logging In

After entering the URL for your storage router, a login page appears. You can log in as monitor or as admin, and you will be asked for your user name and password. See Table 14 for the user name and factory default password to use for the two login options. If you already configured new passwords for the monitor and/or the administrator mode, use them when logging in.

Table 14: Logging into the Web-Based GUI

Login Options	User Name	Factory Default Password
Monitor	monitor	`hp`
Admin	admin	`hp`

Note: If you configured new passwords using the setup wizard or if the SR2122-2 joined an existing cluster with different passwords, use them when logging in.

Monitor Mode

Monitor mode in the web-based GUI will only allow you to monitor the storage router. You cannot configure, maintain, or troubleshoot the storage router in monitor mode. If you click on the Configuration, Maintenance, and Troubleshooting menu items in the GUI, a login dialog box will appear asking for a user name and password for administrator mode.

Administrator Mode

In administrator mode, you can configure, maintain, and troubleshoot the storage router. If you click the Monitor menu item, a login dialog box will appear asking for a user name and password for monitor mode.

Menu Items and Links

The GUI's menu items and links appear horizontally at the top of the browser page. Table 15 lists the menu items and links, the action that takes place when they are clicked, and the login modes from which they are available.

Table 15: Menu and Item Links

Menu Items and Links	Action	Login Mode
Monitor	Lists menu options in left frame to be displayed in main frame.	Monitor only
Configuration	Lists menu options in left frame to be displayed in main frame.	Admin only
Maintenance	Lists menu options in left frame to be displayed in main frame.	Admin only
Troubleshooting	Lists menu options in left frame to be displayed in main frame.	Admin only

Menu Items and Links	Action	Login Mode
Support	Opens the HP.com “Service & Support” page in a new browser window.	Monitor and Admin
Home	Returns to the GUI’s login page where you select to log in as either Monitor or Admin.	Monitor and Admin
Help	Opens the GUI’s online help in a new browser window.	Monitor and Admin

Configuring System Parameters

6

This chapter explains how to configure system parameters on your SR2122-2 storage router and contains the following sections:

System parameters can be configured or changed using CLI commands, as described in this chapter, or via the web-based GUI. To access the web-based GUI, point your browser to the management interface IP address of the storage router. After logging on, click the Help link to access online help for the GUI.

Prerequisite Tasks

Before configuring system parameters, make sure you have finished the following tasks:

- Completed the hardware installation according to the storage router Hardware Installation Guide
- Entered values as requested by the initial system configuration script (for more information, see "Initial System Configuration Script" on page 88)

Note: You do not need to perform the configuration tasks in this chapter if you ran the complete IP Storage Router Setup Configuration Wizard (using the `setup CLI` command with no keyword), or if you ran the wizards separately using all the `setup CLI` commands except `setup scsi`. However you may wish to perform some of the optional configuration procedures described in this chapter such as configuring IP routes or SSH access.

Configuration Tasks

Note: All configuration tasks require Administrator mode access to the storage router.

To configure system parameters on your storage router:

1. Configure the management interface.
2. Configure the time and date.
3. Configure IP routes. (Optional)
4. Configure network management access. (Optional)
5. Configure passwords.
6. Configure administrator contact information. (Optional)
7. Configure the high-availability (HA) interface. (Optional)
8. Configure for Secure Shell (SSH) access. (Optional)
9. Configure for iSNS communications. (Optional)
10. Verify and save configuration.

Note: You can verify and save the configuration (by using the `save system bootconfig or save all bootconfig` command) at any point in the process of performing the configuration tasks.

Figure 45 illustrates the example configuration used in this chapter.

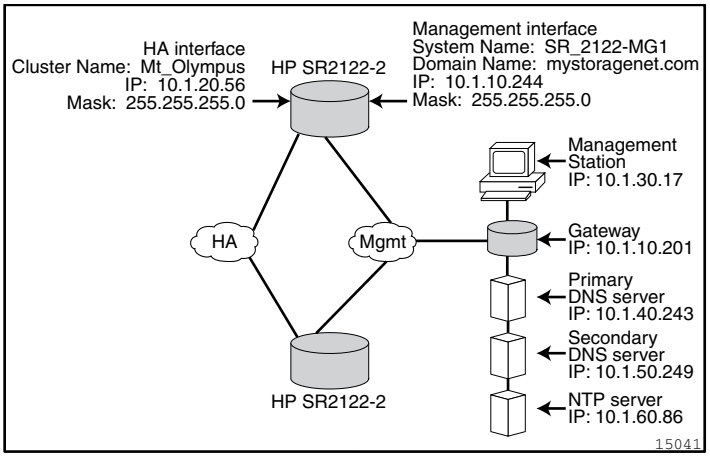


Figure 45: System parameters example configuration

Configuring the Management Interface

Configuring the management interface consists of tasks for setting the system name, IP address and mask, gateway, and DNS servers. Use the following procedure to configure the management interface.

If you want external servers, such as RADIUS, TACACS+, or SMTP servers, to communicate with the SR2122-2 via a specific IP address on a Gigabit Ethernet interface (for in-band management), configure the IP address on the desired Gigabit Ethernet interface as described in Step 4. Save the changes to the bootable configuration (**save all bootconfig**) and then reboot the storage router.

Note: The purpose of Figure 45 is an example system configuration only. The IP addresses and all names given below are examples only.

1. `enable` — Enter Administrator mode
2. `hostname` *`SR_2122-2-MG1`* — Specify or change the system name. The system name identifies the SR2122-2 through the management interface and appears immediately in the prompt.
3. `interface mgmt ip-address` *`10.1.10.224/24`* — Specify or change the IP address and subnet mask for the management interface.

Note: If this storage router is to participate in a cluster, the management interface for all storage routers in the cluster must be on the same IP subnet.

---

4. `interface` *`ge1`* `ip-address` *`10.1.70.85/24`* `secondary` *`ge2`* — (Optional) Configure an IP address and subnet mask on ge1 to be used for SR2122-2 management and maintenance. Specify ge2 as the secondary interface for this IP address. If the Gigabit Ethernet interface ge1 becomes unavailable and ge2 is available, the IP address will become active on ge2.

Note: If you configure a Gigabit Ethernet IP address with a secondary interface, all Gigabit Ethernet IP addresses on the same subnet must also be configured with the same secondary interface.

---

5. `no restrict` *`ge1`* `ssh, no restrict` *`ge2`* `ssh` — (Optional) Configure the Gigabit Ethernet interfaces to be used for management and maintenance for access via the desired protocol(s). In this configuration example, management access to the SR2122-2 through the configured Gigabit Ethernet IP address is allowed for both ge1 and ge2 via Secure Shell (SSH) protocols.
6. `ip name-server` *`10.1.40.243`* — (Optional) Set the primary and secondary DNS IP addresses. Specifies the IP address of the primary DNS server if the management interface IP address is to be correlated with a DNS host name. If there is a secondary DNS the second IP address specifies the IP address of the secondary DNS server.
7. `ip domain-name` *`mystoragenet.com`* — (Optional) Specify the domain name of the storage router. Use this command in conjunction with the `ip name-server` command.

Configuring Time and Date

Configuring time and date parameters consists of specifying the time, date, time zone, and time server. To configure the time and date parameters:

1. `enable` — Enter Administrator mode.
2. `clock timezone` *`US/Pacific`* — Identify the time zone where the storage router is located. If a time zone is not identified, time is assumed to be GMT.
3. `clock set` *`08:20:00 04 15 2002`* — Set time and date (for example: time, 8:20 a.m.; date, April 14, 2002).
4. `ntp peer` *`10.1.60.86`* — (Optional) Specify the name or IP address of the network time protocol (NTP) server with which the storage router will synchronize the date and time.

Note: After a time change, a reboot is required to synchronize the internal FC switch syslog and devlog timestamps.

Configuring IP Routes

If the storage router requires access to any IP address outside the management subnet, you must configure the appropriate routes in the SR2122-2 routing table. You can configure static routes, or if you are using RIP in your network, you can enable the storage router to dynamically learn routes using the routing information protocol (RIP).

When there are multiple routes to the same destination, use administrative distance to determine which route to install in the routing table. The default administrative distance for static routes is 1; the administrative distance for dynamic routes created by RIP is 120. The route with the lower administrative distance is installed in the routing table (as long as the interface used by the route is up).

Note: The SR2122-2-2 can learn a maximum of 200 routes. Additional routes that are received are silently ignored. In the SR2122-2 routing table, a static route will always override a learned route. To modify this behavior, change the administrative distance of a static route to a value greater than 120.

Static Routes

To manually configure the SR2122-2 routing table using static IP routes.

1. `enable` — Enter Administrator mode
2. `ip route` *`10.1.30.0/24 10.1.10.201`* — (Optional) Configure a gateway IP address if the storage router is to be managed from a management station outside the storage router management subnet. The second IP address specifies a gateway on the storage router management network that will provide access to a management station.

Note: In this configuration example, the mask is set to 24 (255.255.255.0) to allow any host on subnet 10.1.30.0 to be a management station.

Dynamic Routes via RIP Listening

Use the `ip rip enable` command to configure the storage router to learn routes from RIP advertisements, and dynamically populate the routing table. The storage router supports both RIP version 1 (v1) and RIP version 2 (v2).

The SR2122-2 RIP implementation runs RIP v2 in broadcast mode. This allows the storage router to learn from either RIP v1 or RIP v2 hosts that are operating in broadcast mode. The storage router will not learn routes from RIP v2 hosts operating in multicast mode.

Note: The storage router is a passive, or silent, RIP device; it updates routes based on RIP advertisements but it does not advertise.

---

1. `enable` — Enter Administrator mode
2. `ip rip enable` — Enable RIP listening. The storage router listens for advertised routes, learning routing information dynamically as it is exchanged in the network.

Configuring Network Management Access

Configuring network management access consists of tasks for configuring SNMP. To configure SNMP for network management access:

1. `enable` — Enter Administrator mode.
2. `no restrict` *`all`* `telnet` — (Optional) Enable Telnet access on **all** interfaces. By default, Telnet access is enabled on only the management interface.
3. `snmp-server community` *`world`* `ro` — (Optional) Specify the name of the community having read-only access of the storage router network (that is, to which community's GET commands the storage router will respond). The default read community is **public**.
4. `snmp-server community` *`mynetmanagers`* `rw` — (Optional) Specify the name of the community having write access to the storage router network (that is, to which community's SET commands the storage router will respond). The default write community is **private**.
5. `snmp-server host` *`10.1.30.17`* `version` *`2`* `traps` — Specify the IP address for the first destination host used for a specified version of notifications (traps). Version 1 traps is the default version.

Note: In this configuration example, the trap hosts have IP addresses that are outside the storage router management subnet. In an earlier step in the "Configuring the Management Interface" section, a gateway was already specified providing access to hosts on the **10.1.30.0** subnet.

---

6. `snmp-server host` *`10.1.30.18`* `traps` — (Optional) Specify the IP address for the second destination host used for notifications (traps). Version 1 traps is the default version.
7. `snmp-server sendauthtraps` — (Optional) Enable sending of authentication failure traps.
8. `no snmp-server linkupdown all` — (Optional) By default, the SNMP agent is enabled to generate link up/down traps for all interfaces. In this configuration example, the command disables this setting for all interfaces.

Configuring Passwords

Configuring passwords consists of setting the monitor-mode and administrator-mode passwords for access to the 10/100 Ethernet management interface (used for the CLI via Telnet and the web-based GUI via HTTP). You can enable these passwords to restrict access to the EIA/TIA-232 console interface. To configure passwords:

Note: The factory default password for both Monitor and Administrator modes is `hp`.

In a cluster environment, passwords are cluster-wide configuration elements and apply to all storage routers in a cluster. All password management functions are handled by a single storage router. If you issue try to set the Administrator or Monitor mode passwords from a storage router that is not performing password management functions, the CLI displays an informational message with the name of the storage router that is currently handling those functions.

To configure passwords

1. `enable` — Enter Administrator mode.
2. `monitor password` *`janu$01`* — Set the monitor password (for user who only monitors storage router operation).
3. `admin password` *`elect@50`* — Set the administrator password (for system administrators, allowing configuration changes).
4. `restrict console` — (Optional) Enable the Monitor-mode and Administrator-mode passwords to be required when accessing the SR2122-2 via a console connected to the EIA/TIA-232 console interface.

Configuring Administrator Contact Information

Configuring administrator contact information consists of tasks for specifying the name, e-mail address, phone number, and pager number of the system administrator for the storage router. To configure administrator contact information:

1. `enable` — Enter Administrator mode.
2. `admin contactinfo name "PatJ. Smith" email pjsmith@mystoragenet.com phone "763 555-117" pager "763 555-7766"` — Provide contact name, email address, phone number, and pager number. Enclose each string that contain spaces in single or double quotes.

Note: The admin contactinfo command requires that you specify either one parameter or all four parameters.

Configuring the High-Availability Interface

When the storage router is part of a storage router cluster, you will need to configure the high availability (HA) interface. To configure the HA interface parameters:

1. `enable` — Enter Administrator mode.
2. `interface ha ip-address 10.1.20.56/24` — Specify or change the IP address and subnet mask for the HA interface

See Chapter 11, "Configuring a High Availability Cluster" for more information about configuring the SR2122-2 in a high availability cluster.

Configuring for Secure Shell (SSH) Access

The SR2122-2 Storage Router supports Secure Shell (SSH) as an alternative to Telnet protocol for SR2122-2 management. SSH provides encryption and strong authentication for interactive SR2122-2 management sessions. The SR2122-2 supports SSH protocol version 2 and allows port forwarding.

The SR2122-2 SSH implementation supports execution of interactive commands only; non-interactive commands cannot be executed. Secure FTP (sftp) and Secure Copy (scp) are not supported.

SSH is enabled for the SR2122-2 and the SSH service is started, by default. However, you must generate a public/private key pair for the SR2122-2 before you can use SSH to establish a management session. By default, SSH is restricted on all interfaces except the management interface.

To configure the SR2122-2 to use SSH.

1. `enable` — Enter Administrator mode.
2. `show ssh` — Display the status of the SSH service for the SR2122-2. The SSH service is running and is enabled by default. See Example 1.
3. `ssh enable` — (Optional) If SSH is not enabled, start the SSH service.
4. `ssh keygen` — Generate the SSH public/private key pair using the specified number of bits. For example, generate a 1024-bit key pair (the default setting).
5. `show restrict` — Display the current protocol restrictions for the SR2122-2. Verify that SSH is enabled for the required interface.
6. `no restrict` *`mgmt`* `ssh` — (Optional) Enable SSH for the required interfaces. For example, enable SSH for the SR2122-2 management interface.
7. `restrict` *`mgmt`* `telnet` — (Optional) If SSH is being used as a replacement for Telnet, you can disable Telnet access through the specified SR2122-2 interface (or all interfaces). For example, disable Telnet access via the management interface.
8. `no telnet enable` — (Optional) You can also disable Telnet for the entire SR2122-2 by stopping the Telnet service.

Example 1: Example: Results of "show ssh" Command

```
[SR2122-2]# show ssh
SSH Server Configuration
               Status: enabled
```

Configuring for iSNS Communications

Internet Storage Name Service (iSNS) is an IETF standard that facilitates scalable configuration and management of iSCSI and FC storage devices in an IP network, by providing a set of services comparable to that available in FC networks. Using the iSNS, each storage device subordinates its discovery and management responsibilities to the iSNS server.

The SR2122-2 functions as an iSNS client. SCSI routing instances are registered as iSNS entities, targets are registered as storage nodes, and SCSI routing instance server interface IP addresses are registered as network portals with the iSNS server. The storage router management interface IP address is registered as an attribute of the SCSI routing instance iSNS entity.

iSNS servers may use TCP or UDP for client registrations and other communications. You can configure the storage router to use either protocol type to the identified iSNS server.

To configure the storage router for iSNS communications:

1. `enable` — Enter Administrator mode.
2. `isns enable tcp server` *`10.1.70.43`* — Enable TCP communications and client registrations to the iSNS server at the specified IP address.

Verifying and Saving Configuration

Verify the system parameters using the following procedure. You can save the configuration at any time using either the `save system bootconfig` or `save all bootconfig` commands. You must save the running configuration to the bootable configuration for it to be retained in the storage router when it is rebooted.

To verify configuration information.

1. `show system` — Display system information, such as system name, software version, date and time (including time zone), NTP server, DNS (name server), and management and HA interface IP addresses.
2. `show ip route` — (Optional) Display the system route table, if you added any routing information, or if you enabled the storage router for RIP listening.
3. `show ip rip` — (Optional) Display RIP configuration and operational information, if set.
4. `show snmp` — (Optional) Display SNMP management configuration information for the storage router, if set.
5. `show admin` — (Optional) Display contact information for the system administrator of the storage router, if set.
6. `show ssh` — (Optional) Display SSH operational status, if configured.
7. `show ssh fingerprint` — (Optional) Display public key information for the ssh, if set.
8. `show restrict` — (Optional) Display the restrict settings, if you make changes to the protocols allowed for the various SR2122-2 interfaces.
9. `show isns` — (Optional) Display iSNS configuration information.
10. `show bootconfig` — (Optional) Display the current boot configuration of the SR2122-2.
11. `show runningconfig` — (Optional) Display the current running configuration of the SR2122-2.

Configuring VLAN

7

This chapter explains how to configure your SR2122-2 storage router for a virtual local area network (VLAN) and contains the following sections:

You can configure for VLAN using CLI commands as described in this chapter or via the web-based GUI. To access the web-based GUI, point your browser to the management interface IP address of the storage router. After logging on, click the Help link to access online help for the GUI.

Prerequisite Tasks

Before configuring for VLAN, make sure you have configured all system parameters as described in Chapter 5, "Configuring the Storage Router" or Chapter 6, "Configuring System Parameters"

VLAN Encapsulation

The storage router uses the IEEE 802.1Q standard for VLAN encapsulation.

Note: If the storage router is connected to a switch, the switch port must be configured as a trunk port and the encapsulation set to 802.1Q, not Inter-Switch Link (ISL), which is the default setting for trunk ports.

Configuration Tasks

To configure for VLAN on the storage router:

1. Configure for VLAN using the VLAN Trunking Protocol (VTP) or Configure for VLAN without using VTP.
2. Configure an IP route.
3. Verify and save configuration.

Note: You can verify and save the configuration at any point in the process of performing the configuration tasks. Save your configuration by using the `save all bootconfig` CLI command. This command saves all configuration data to the bootable configuration, which is then used when the storage router is rebooted.

4. Proceed to Chapter 8, "Configuring SCSI Routing" to configure SCSI routing and to assign a VLAN to a SCSI routing instance.

Figure 46 contrasts configuring the storage router for VLAN with VTP and without VTP.

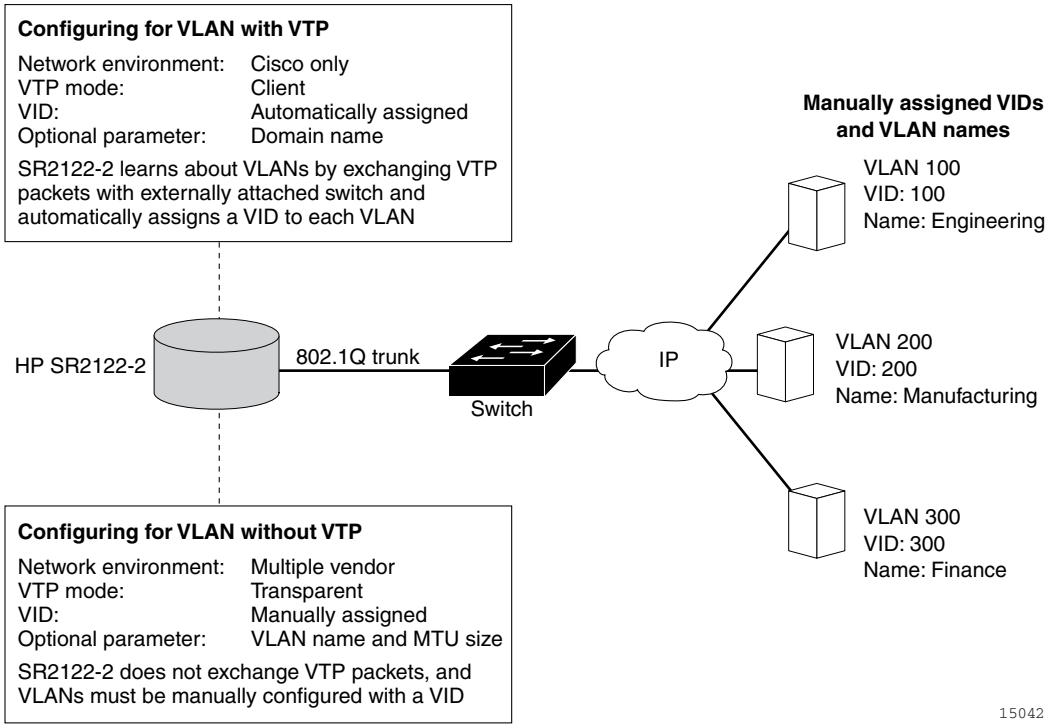


Figure 46: Contrast of configuring for VLAN with VTP and without VTP

Configuring for VLAN with VTP

Configuring for VLAN using the VLAN Trunking Protocol (VTP) consists of assigning the VTP domain name and setting the VTP mode to client. VTP, a proprietary protocol of Cisco Systems, is used to propagate VLAN information around a switched network.

To configure VLAN using VTP:

Note: VTP can only be used in a Cisco network environment.

---

1. `enable` — Enter Administrator mode.
2. `vtp domain` *`opus`* — Assign a VTP domain name opus to which the storage router belongs. If a domain name is not specified, the storage router will assign itself to the first domain from which it receives a VTP message. The default setting is **none**.
3. `vtp mode` *`client`* — The default setting for the VTP mode is **client**. Set the VTP mode to **client** if the current setting is **transparent**.

   In client mode, the storage router will exchange VTP packets with an externally attached switch to learn about the VLANs that are accessible in the network.

Note: The VTP mode is a cluster-wide configuration item. When set by the user and saved, the mode setting becomes active on all storage routers in the cluster.

Configuring for VLAN without VTP

Configuring for VLAN without using VTP consists of setting the VTP mode to transparent, assigning a VID, and optionally assigning a name and maximum transmission unit (MTU) size to the VLAN.

To configure VLAN without using VTP:

1. `enable` — Enter Administrator mode.
2. `vtp mode` *`transparent`* — Set the VTP mode for the storage router to **transparent**. In transparent mode the storage router does not exchange VTP packets and VLANs must be manually configured. The default setting is **client**.

Note: The VTP mode is a cluster-wide configuration item. When set by the user and saved, the mode setting becomes active on all storage routers in the cluster.

---

3. `vlan` *`100`* `or vlan` *`100`* `name` *`Engineering`* `and mtusize` *`9000`* — Assign a VLAN identifier VID number that uniquely identifies the VLAN. The VID can be any integer from 1 to 4095.

   Optionally, a VLAN can be assigned a unique name **Engineering** up to 32 characters in length. If a name is not specified, a default name is **automatically assigned**. The default name has VLAN as the prefix followed by the VID, left padded to four bytes (for example, **VLAN0100**).

   Optionally, an MTU size can be specified using a value from 1500 to 9000. The default value is **1500**.

Note: VLANs are a cluster-wide configuration item. When set by the user and saved, the VLAN information is propagated to all storage routers in the cluster.

Configuring an IP Route

Configuring an IP route to access the VLAN consists of specifying a static route that uses a gateway attached to the desired VLAN. To configure an IP route.

1. `enable` — Enter Administration mode.
2. `ip route` *`10.2.90.285/32 10.2.10.233`*`, interface` *`ge2`*`, and VLAN` *`100`* — Specify the IP address and subnet mask 10.2.90.285/32 of the destination. Set the subnet mask to **255.255.255.255**. In this example the subnet mask was set using CIDR style /32.

   In addition, specify the gateway IP address 10.2.10.233, the interface name ge2, and the VID 100.

Note: To find the desired VID number, use the `show vlan` command. VIDs are listed in the VLAN column.

Verifying and Saving Configuration

Verify VTP and VLAN operational and configuration information using the procedures that follow. You can save the configuration at any time by using the `save all bootconfig` command. You must save the running configuration to the bootable configuration for it to be retained in the storage router when it is rebooted. Once you have saved the configuration, you can verify that the configuration to be used when the storage router is rebooted matches the currently running configuration.

To verify VTP operational information:

1. `enable` — Enter Administration mode.
2. `show vtp` — Display VTP operational information (Example 2).

Example 2: Verifying VTP Operational Information

```
[Storage Router]# show vtp
Configuration Revision   : 8
Number of existing VLANs : 4
VTP Operating Mode       : Client
VTP Domain Name          : opus
```

To verify VTP configured settings.

1. `enable` — Enter Administration mode.
2. `show vtp config` — Display VTP configured settings (Example 3).

Example 3: Verifying VTP Configured Settings

```
[Storage Router]# show vtp config
vtp mode client
vtp domain opus
```

To verify current operational information for all VLANs either learned from the network using VTP in client mode or configured locally while in transparent mode.

1. `enable` — Enter Administration mode.
2. `show vtp` — Display current VLAN operational information (Example 4).

Example 4: Verifying VLAN Operational Information

```
[Storage Router]# show vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -----
100  Engineering                       active    ge2
200  Manufacturing                     active    ge2

VLAN Type  MTU   Interfaces
---- ----- ----- --------------------------------
100  enet  1500  ge2VLAN100
200  enet  1500  ge2VLAN200
```

To verify configured VLAN information.

1. `enable` — Enter Administration mode.
2. `show vtp config` — Display VTP configured information (Example 5).

Example 5: Verifying VLAN Configuration Information

```
[Storage Router]# show vlan config
vlan 100 name Engineering mtu 1500
vlan 200 name Manufacturing mtu 1500
```

Assigning a VLAN to a SCSI Routing Instance

Assigning a VLAN to a SCSI routing instance is achieved with the `scsirouter serverif vlan` command. This procedure is provided in the "Configuring a Server Interface" section of Chapter 8, "Configuring SCSI Routing" HP recommends that you follow the configuration tasks to configure SCSI routing in the order given in that chapter at the time you are ready to configure SCSI routing.

Configuring SCSI Routing

8

This chapter explains how to configure your SR2122-2 storage router for SCSI routing and contains the following sections:

SCSI routing can be configured using CLI commands as described in this chapter or via the web-based GUI. To access the web-based GUI, point your browser to the storage router management interface IP address. After logging on, click the Help link to access online help for the GUI.

Prerequisite Tasks

Before configuring SCSI routing, make sure you have configured all system parameters as described in Chapter 5, "Configuring the Storage Router" or Chapter 6, "Configuring System Parameters"

If the VLAN service is to be used with the storage router, configure VLANs as described in Chapter 7, "Configuring VLAN" before proceeding.

Configuration Tasks

To configure SCSI routing on your storage router:

1. Create a SCSI routing instance. Once an instance is created, you will configure that instance with parameters for a server interface, iSCSI targets, and access by IP hosts.
2. Configure the server interface with or without VLAN.
3. Configure iSCSI targets.
4. Configure an access list that identifies which IP hosts can access iSCSI targets configured as part of a SCSI routing instance. An access list is necessary if you want to specify access to iSCSI targets on a per-IP host basis. An access list is not necessary if you want to specify that all IP hosts have access to the iSCSI targets configured in a SCSI routing instance. (Optional)
5. Configure access. This identifies which IP hosts can access the iSCSI targets configured as part of a SCSI routing instance.
6. Verify and save configuration.

Note: Although this is shown as the last step, you can verify and save the configuration at any point in the process of performing the configuration tasks. Save your configuration by using the `save all bootconfig` CLI command. This command saves all configuration data to the bootable configuration, which is then used when the storage router is rebooted.

Caution: When making changes to a SCSI routing instance (such as adding or deleting targets or changing access) be sure to make the complementary changes to the iSCSI driver configuration of IP hosts that use that SCSI routing instance to access the storage resources. See the "Installing the iSCSI Drivers" section of Chapter 5, or the readme files for the appropriate iSCSI drivers for additional details. (You can access the latest iSCSI drivers and readme and example configuration files from http://www.hp.com/support).

Figure 47 illustrates SCSI routing configuration elements and Figure 48 illustrates the example configuration used in this chapter. Figure 49 illustrates how the configuration of SCSI routing instances determines VLAN access to storage devices.

Note: Configuring the SCSI routing instance does not include configuring the FC interfaces. Once the SCSI routing instance is configured, all the FC interfaces are available. For more information on the FC interfaces default characteristics, see the "Default Values For FC Interfaces" section on page 136.

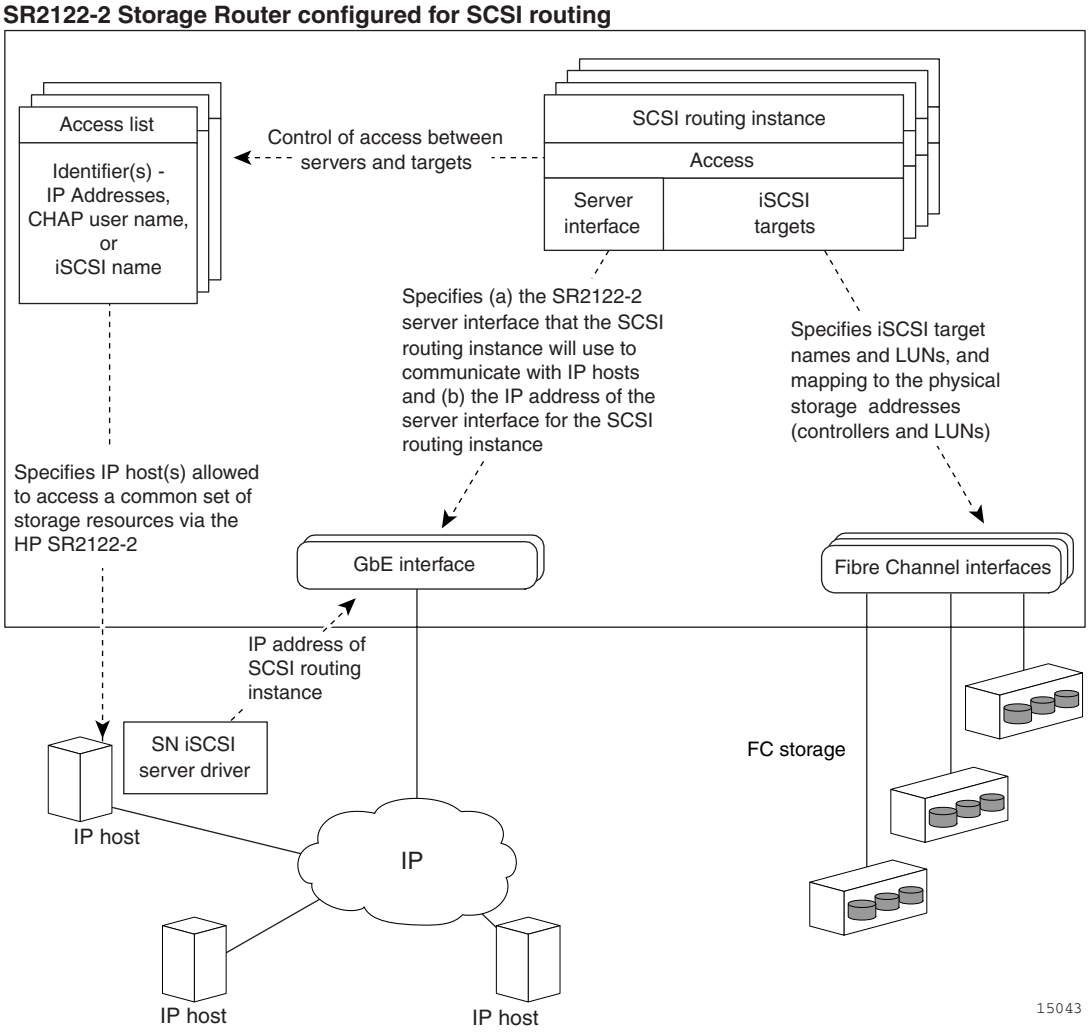


Figure 47: Configuration elements for SCSI routing

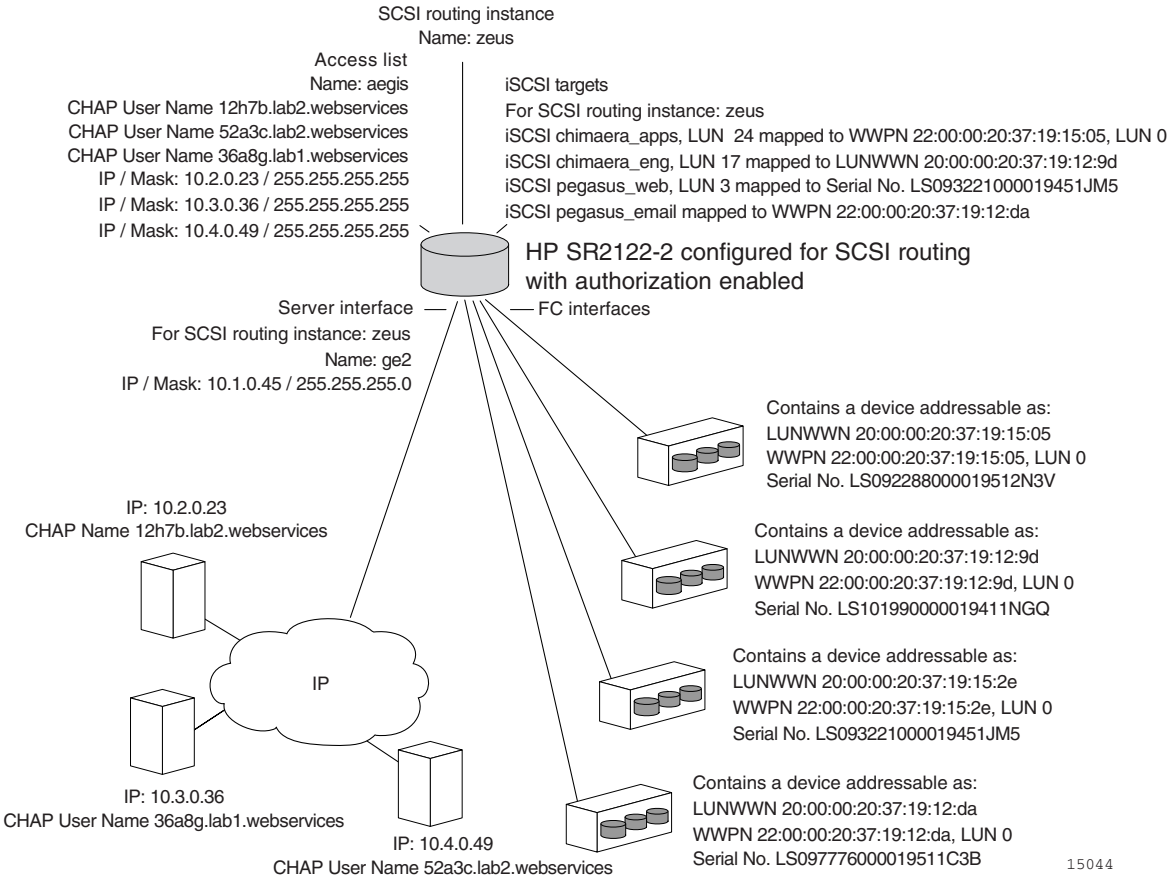


Figure 48: SCSI routing parameters example configuration

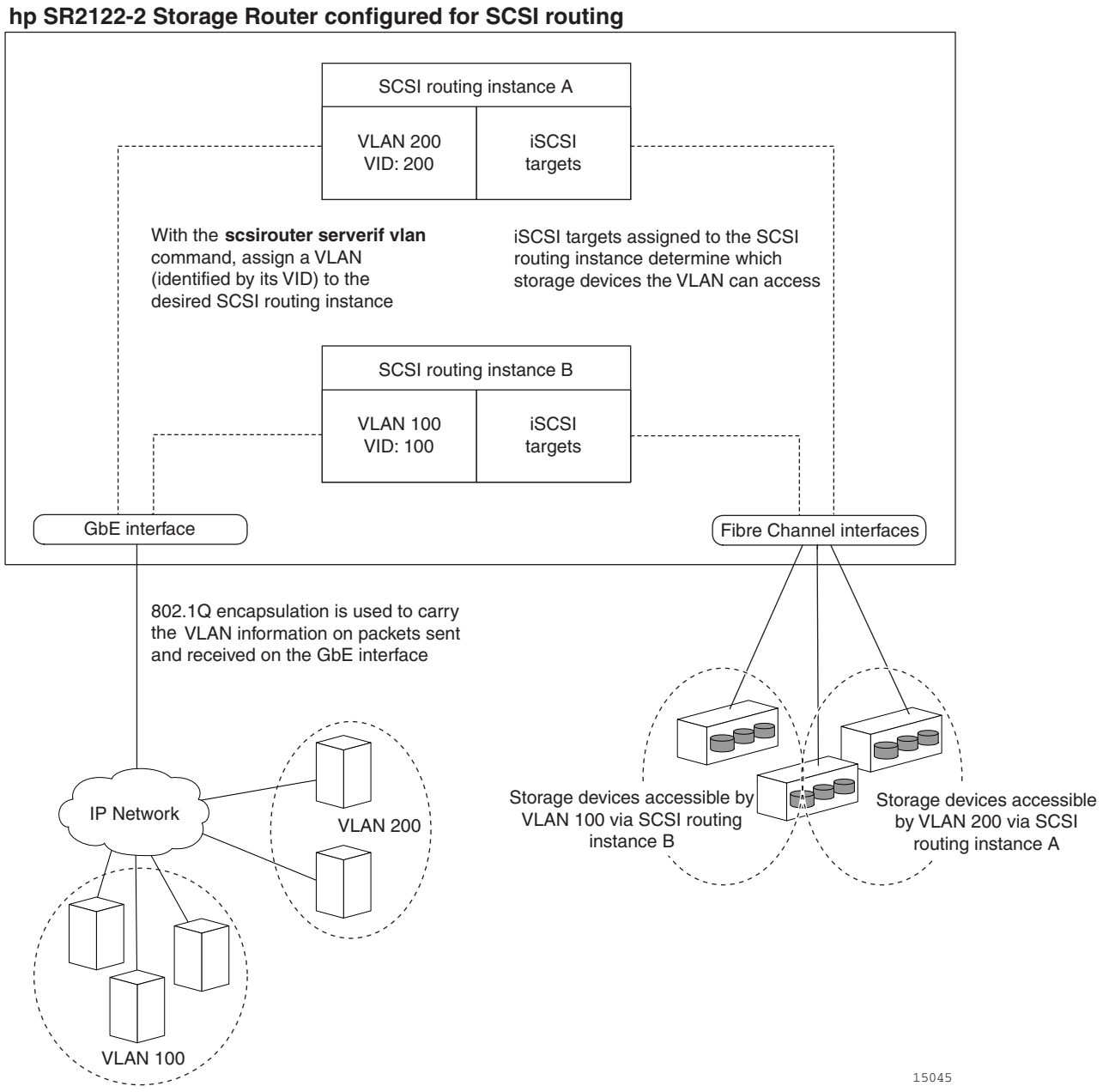


Figure 49: Configuration of SCSI routing determines VLAN access to storage

Creating a SCSI Routing Instance

Creating a SCSI routing instance consists of naming the new instance. To create a SCSI routing instance:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* — Create a SCSI routing instance by naming the new instance **zeus**.

Note: You can define up to 12 instances on a single storage router or across a cluster. For additional details about configuring storage router clusters for high availability, see Chapter 11, "Configuring a High Availability Cluster"

Configuring a Server Interface

Configuring a server interface consists of assigning a server interface along with an IP address and subnet mask to the desired SCSI routing instance. If the storage router is to be used with VLAN, specify the VLAN by its VID.

Without VLAN

To configure a server interface for a SCSI routing instance:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `serverif` *`ge2`* `VLAN` *`100 10.1.0.45/24`* — Assign a server interface `ge2` to the desired SCSI routing instance **zeus**. Specify the IP address and subnet mask **10.1.0.45/24** that IP hosts will use to access the SCSI routing instance. In this example, the subnet mask of **255.255.255.0** was set using CIDR style **/24**.

With VLAN

To assign a server interface and VLAN to a SCSI routing instance:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `serverif` *`ge2`* `VLAN` *`100 10.1.0.45/24`* — Assign a VLAN, identified by its VID **100**, to the desired SCSI routing instance **zeus**. Specify the server interface **ge2** and the IP address and subnet mask **10.1.0.45/24** that the VLAN will use to access the SCSI routing instance. In this example, the subnet mask of **255.255.255.0** was set using CIDR style **/24**.

Note: To look up the VID, use the `show vlan` command. VIDs are listed in the VLAN column.

Configuring iSCSI Targets

Configuring iSCSI targets consists of specifying the SCSI routing instance to which an iSCSI target is to be assigned, specifying the iSCSI target, and mapping the iSCSI target to a physical storage device. When assigning an iSCSI target, you can specify the physical storage device either by physical storage address, serial number, or by an index number assigned to the device.

Note: When a new iSCSI target is configured, IP hosts do not have access to it. You need to configure access to newly created iSCSI targets according to the "Configuring Access" section later in this chapter.

Use the procedures that follow according to mapping type and storage addressing type:

- Target-and-LUN mapping using WWPN addressing
- Target-and-LUN mapping using LUNWWN addressing
- Target-and-LUN mapping using Serial Number addressing
- Target-only mapping using WWPN addressing

Example 6: Indexed List of Storage Devices

```
id interface lunwwn           wwpn             tgtid lun
vendor  product    serial number

1  fc4       20000020371912d5 22000020371912d5 n/a   0   DEC
    HSG80      LS099969000019511C2H
2  fc4       20000020371912da 22000020371912da n/a   0   DEC
    HSG80      LS097776000019511C3B
3  fc4       200000203719129d 220000203719129d n/a   0   DEC
    HSG80CCL   LS101990000019411NGQ
4  fc4       2000002037191505 2200002037191505 n/a   0
  COMPAQ  MSA1000    LS101990000019451JM5
5  fc4       20000020371912b2 22000020371912b2 n/a   0
  COMPAQ  MSA1000    LS099843000019430RC7
6  fc4       200000203719152e 220000203719152e n/a   0
  COMPAQ  MSA1000    LS093221000019451JM5
```

Target-and-LUN mapping using WWPN addressing

To map iSCSI targets to storage devices by physical storage address:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `target` *`chimaera_apps`* `LUN` *`24`* `WWPN` *`22:00:00:20:37:19:15:05`* `LUN` *`0`* — Specify desired SCSI routing instance **zeus**. Specify iSCSI target **chimaera_apps** and LUN **24**, and map it to the desired physical address WWPN **22:00:00:20:37:19:15:05** LUN **0**.

To map iSCSI targets to storage devices by an index number:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `target` *`chimaera_apps`* `LUN` *`31`* `WWPN` *`#?`* — Specify desired SCSI routing instance **zeus**. Specify iSCSI target **chimaera_apps** and LUN **31**, and prompt for an indexed list of available storage addresses using the number sign and a question mark **#?**.
3. `SCSIRouter` *`zeus`* `target` *`chimaera_apps`* `LUN` *`31`* `WWPN` *`#4`* — Choose a physical address designated by an index number (see index number 4 in Example 6) to map the iSCSI target **chimaera_apps** and LUN **31** combination to the desired physical address WWPN **22:00:00:20:37:19:15:05**, LUN **0**.

Target-and-LUN mapping using LUNWWN addressing

To map iSCSI targets to storage devices by physical storage address:

1. `enable` — Enter Administration mode.
2. `SCSIRouter zeus target chimaera_apps LUN 17 LUNWWN 22:00:00:20:37:19:12:9d` — Specify desired SCSI routing instance **zeus**. Specify iSCSI **target chimaera_apps** and LUN **17**, and map it to the desired physical address LUNWWN **22:00:00:20:37:19:12:9d.**

To map iSCSI targets to storage devices by an index number:

1. `enable` — Enter Administration mode.
2. `SCSIRouter zeus target chimaera_apps LUN 17 WWPN #?` — Specify desired SCSI routing instance **zeus**. Specify iSCSI target **chimaera_apps** and LUN **17**, and prompt for an indexed list of available storage addresses using the number sign and a question mark **#?**.
3. `SCSIRouter zeus target chimaera_apps LUN 17 LUNWWN #3` — Choose a physical address designated by an index number (see index number 3 in Example 6) to map the iSCSI target **chimaera_apps** and LUN **17** combination to the desired physical address LUNWWN **22:00:00:20:37:19:12:9d**.

Target-and-LUN mapping using Serial Number addressing

To map iSCSI targets to storage devices by serial number:

1. `enable` — Enter Administration mode.
2. `SCSIRouter zeus target pegasus_web LUN 3 serial number LS093221000019451JM5` — Specify desired SCSI routing instance **zeus**. Specify iSCSI target **pegasus_web** and LUN **3**, and map it to the desired serial number **LS093221000019451JM5.**

To map iSCSI targets to storage devices by an index number:

1. `enable` — Enter Administration mode.
2. `SCSIRouter zeus target pegasus_web LUN 3 serial number #?` — Specify desired SCSI routing instance **zeus**. Specify iSCSI target **pegasus_web** and LUN **3**, and prompt for an indexed list of available storage addresses using the number sign and a question mark **#?**.

3. `SCSIRouter zeus target pegasus_web LUN 3 serial number #6` — Choose a physical address designated by an index number (see index number 6 in Example 6) to map the iSCSI target **pegasus_web** and LUN **3** combination to the desired physical address serial number **LS0932210000019451JM5**.

Target-only mapping using WWPN addressing

To map iSCSI targets to storage devices by physical storage address:

1. `enable` — Enter Administration mode.
2. `SCSIRouter zeus target pegasus_email WWPN 22:00:00:20:37:19:12:da` — Specify desired SCSI routing instance **zeus**. Specify iSCSI target **pegasus_email**, and map it to the desired physical address WWPN **22:00:00:20:37:19:12:da** and any LUNs available as part of that WWPN.

To map iSCSI targets to storage devices by index numbers:

1. `enable` — Enter Administration mode.
2. `SCSIRouter zeus target pegasus_email WWPN #?` — Specify desired SCSI routing instance **zeus**. Specify iSCSI target **pegasus_email** and prompt for an indexed list of available storage addresses using the number sign and a question mark **#?**.
3. `SCSIRouter zeus target pegasus_email WWPN #2` — Choose a physical address designated by an index number (see index number 2 in Example 6) to map the iSCSI target **pegasus_email** to the desired physical address WWPN **22:00:00:20:37:19:12:da.**

Configuring an Access List

Configuring an access list consists of creating an access list by naming it and identifying the IP hosts that have permission to access storage devices via iSCSI target names. IP hosts can be identified by:

- IP address
- CHAP user name (used for iSCSI authentication)
- iSCSI name of the IP host — The iSCSI name is a UTF-8 character string based on iSCSI functional requirements. It is a location-independent permanent identifier for an iSCSI node, and is generated when a target is initially created.

An access list can contain one or more types of identification entries. If an identification entry type exists in the access list, the IP host attempting to access the associated storage target must have a matching entry defined in the access list. For example, if an access list contains both IP address and iSCSI name identification entry types, then every IP host that requires access to the associated set of storage resources must have a matching IP address and iSCSI name entry in the access list.

An access list is necessary if you want to specify access to iSCSI targets on a per-IP host basis. An access list is not necessary if you want to specify that all IP hosts have access to the iSCSI targets configured in a SCSI routing instance.

Note: If there is a CHAP user name entry in the access list, the SCSI routing instance used to access the storage target must also have iSCSI authentication enabled. See Chapter 10, "Configuring Authentication" for additional information about AAA and iSCSI authentication.

Use the following procedure to create an access list. In this procedure, the access list is called **aegis** and the IP host identifiers include three IP addresses (**10.2.0.23**, **10.3.0.36**, and **10.4.0.49**) and a CHAP-username (**12h7b.lab2.webservices**):

1. `enable` — Enter Administration mode.
2. `accesslist aegis` — Create an access list by naming it **aegis**. There is a 31 character limit.
3. `accesslist aegis description "Access to zeus SCSI routing service"` — Add a string as a description for the access list. Enclose the string using single or double quotes. (Optional)
4. `accesslist aegis 10.2.0.23/32 10.3.0.36/32 10.4.0.49/32` — Add IP addresses of IP hosts to the access list. Separate multiple IP addresses with a space. To limit the access to each IP address, set the subnet mask to **255.255.255.255**. In this example, the subnet mask was set using CIDR style **/32**.
5. `accesslist aegis CHAP-username 12h7b.lab2.webservices` — Add CHAP-usernames in the access list. To limit the access to each CHAP-username. The password it supplies must be successfully validated using the AAA method configured.

Note: Authentication must be enabled when using CHAP-usernames in the access list.

Note: In a cluster environment, all access lists must be created and maintained on the first storage router to join the cluster. If you issue the `accesslist` commands from another storage router in the cluster, the CLI displays an informational message with the IP address of the storage router that is currently handling all access list functions. For more information on operating the storage router in a cluster, see Chapter 12, "Maintaining and Managing the Storage Router"

Configuring Access

Configuring access consists of specifying which iSCSI targets can be accessed by IP hosts. When configuring access, you can specify one iSCSI target at a time or all iSCSI targets. Similarly, you can specify one access list at a time or all IP hosts using a SCSI routing instance. In addition, you can deny access to iSCSI targets one at a time or all at once.

The default for access to newly configured iSCSI targets is none. You must configure access according to the information provided in this section.

Use the procedures that follow according to the type of access:

- Access an iSCSI target by IP hosts identified in an access list
- Access an iSCSI target by all IP hosts
- Access all iSCSI targets by IP hosts identified in an access list
- Access all iSCSI targets by all IP hosts
- Access denied to one iSCSI target
- Access denied to all iSCSI targets

Access an iSCSI target by IP hosts identified in an access list

To specify one iSCSI target at a time to be accessible by IP hosts listed in an access list:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `target` *`chimaera_email`* `accesslist` *`aegis`* — Specify that an iSCSI target **chimaera_email**, configured as part of a SCSI routing instance **zeus**, can be accessed by IP hosts listed in an access list **aegis**.

Access an iSCSI target by all IP hosts

To specify one iSCSI target at a time to be accessible by all IP hosts.:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `target` *`chimaera_apps`* `accesslist` *`all`* — Specify that an iSCSI target **chimaera_apps**, configured as part of a SCSI routing instance **zeus**, can be accessed by **all** IP hosts.

Access all iSCSI targets by IP hosts identified in an access list

To specify all iSCSI targets to be accessible by IP hosts listed in an access list:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `target` *`all`* `accesslist` *`aegis`* — Specify that **all** iSCSI targets that were configured as part of a SCSI routing instance **zeus**, can be accessed by IP hosts listed in an access list **aegis**.

Access all iSCSI targets by all IP hosts

To specify all iSCSI targets to be accessible by all IP hosts:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `target` *`all`* `accesslist` *`all`* — Specify that **all** iSCSI targets that were configured as part of a SCSI routing instance **zeus** can be accessed by **all** IP hosts.

Access denied to one iSCSI target

To deny access by IP hosts to one iSCSI target at a time:

1. `enable` — Enter Administration mode.
2. `SCSIRouter zeus target` *`chimaera_apps`* `accesslist` *`none`* — Specify that **no** IP host can access the iSCSI target **chimaera_apps**, configured as part of the specified SCSI routing instance **zeus**.

Access denied to all iSCSI targets

To deny access by all IP hosts to all iSCSI targets at once:

1. `enable` — Enter Administration mode.
2. `SCSIRouter` *`zeus`* `target` *`all`* `accesslist` *`none`* — Specify that **no** IP hosts can access **any** iSCSI targets that were configured as part of the specified SCSI routing instance **zeus**.

Verifying and Saving Configuration

Verify the access list configuration and the SCSI routing configuration using the procedures that follow. You can save the configuration at any time by using the `save all bootconfig` command. You must save the running configuration to the bootable configuration for it to be retained in the storage router when it is rebooted. Once you have saved the configuration, you can verify that the configuration to be used when the storage router is rebooted matches the currently running configuration.

To verify access list configuration:

1. `enable` — Enter Administration mode.
2. `Show accesslist` — Display a list of **all** existing access lists (Example 7).
3. `Show accesslist` *`aegis`* — Display the IP host identifies in an access list (Example 8).

Example 7: Verifying Existence of an Access List

```
[SR2122]# show accesslist
aegis
hris-mgmt
```

Example 8: Verifying IP Addresses in an Access List Named aegis

```
[SR2122]# show accesslist aegis
accesslist aegis description "Access to zeus SCSI routing
service"
accesslist aegis 10.2.0.23/255.255.255.255
accesslist aegis 10.3.0.36/255.255.255.255
accesslist aegis 10.4.0.49/255.255.255.255
accesslist aegis chap-username 12h7b.lab2.webservices
```

To verify the configuration of a SCSI routing instance:

1. `enable` — Enter Administration mode.
2. `Show scsirouter` *`zeus`* — Display the parameters configured for the specified SCSI routing instance (Example 9).

Example 9: Verifying Configuration for a SCSI Routing Instance

```
[SR2122]# show scsirouter zeus
zeus description "(not set)"
zeus authenticate "none"
zeus primary "none"
zeus proxy server disabled
zeus failover primary "none"
zeus failover secondary "none"
zeus target naming authority "none"
zeus target log level is not available
zeus target chimaera_apps description "(not set)"
zeus target chimaera_apps Name
"iqn.1987-05.com.hp.00.d3f8a650c7deacecd97e1812d.chimaera_"
zeus target chimaera_apps enabled "TRUE"
zeus target chimaera_apps accesslist "all"
zeus target chimaera_apps lun 24 wwpn
"22:00:00:20:37:19:15:05" lun "0" I/F fci1
zeus target chimaera_eng description "(not set)"
zeus target chimaera_eng enabled "TRUE"
zeus target chimaera_eng accesslist "all"
zeus target chimaera_eng lun 17 lunwwn
"22:00:00:20:37:19:12:9d" I/F fci1
zeus target pegasus_web description "(not set)"
zeus target pegasus_web Name
"iqn.1987-05.com.hp.00.d6bf2b11ed9c88ce9299ea3f0961ad94.pega
sus_web"
zeus target pegasus_web enabled "TRUE"
zeus target pegasus_web accesslist "all"
zeus target pegasus_web lun 3 serial "LS0932210000019451JM5"
I/F fci1
```

Default Values For FC Interfaces

The following are the default operational characteristics for the Fibre Channel interfaces 1 and 2:

- Fairness disabled (switch has priority)
- Automatically negotiated transfer rate (linkspeed auto)
- Multi-Frame sequence bundling enabled
- Automatic selection of port type as:
  - Loop
  - Point-to-point

Configuring FCIP

9

This chapter explains how to configure your SR2122-2 Storage Router for FCIP and contains the following sections:

- Prerequisite Tasks
- Configuration Tasks
- Creating an FCIP Instance
- Assigning an IP Address
- Assigning a Peer Name and Peer IP Address
- Configuring Operational Parameters
- Verifying and Saving Configuration

FCIP is configured in the setup wizard. To configure the FCIP deployment option further and to verify the configuration you can use the procedure in this chapter or you can use the web-based GUI. To access the web-based GUI, point your browser to the management interface IP address of the storage router. After logging on, click the Help link to access online help for the GUI.

For guidance on choosing the correct configuration for your storage situation, please refer to Appendix E, "Recommended Host/Storage Configurations."

Prerequisite Tasks

Before performing FCIP configuration tasks on the SR2122-2, make sure you have configured all system parameters as described in Chapter 5, "Configuring the Storage Router," and Chapter 6, "Configuring System Parameters."

To configure an FCIP instance, you will need the IP address of the FCIP instance on the peer system (another SR2122-2 Storage Router configured for FCIP).

Configuration Tasks

To configure FCIP on an SR2122-2 Storage Router:

1. Create an FCIP instance.
2. Assign an interface and IP address to the FCIP instance for use by the peer system (another SR2122-2 Storage Router configured for FCIP).
3. Assign FCIP peer IP address.
4. (Optional) Configure operational parameters as needed.
5. Verify and save configuration.

Note: Although this is shown as the last step, you can verify and save the configuration at any point in the process of performing the configuration tasks. Save your configuration by using the `save all bootconfig` CLI command. This command saves all configuration data to the bootable configuration, which is then used when the storage router is rebooted.

Creating an FCIP Instance

Creating an FCIP instance consists of naming the new instance. To create an FCIP instance:

1. `enable` — Enter Administrator mode.
2. `fcip` *`fcip1`* — Create an FCIP instance by naming the new instance. For example, name the instance fcip1.

   The FCIP instance named fcip1 uses the Gigabit Ethernet interface ge1; the instance named fcip2 uses ge2. See the *IP Storage Router Command Line Interface Reference Guide* for more information about the `fcip` command.
3. `fcip fcip1 description "Access to SAN island 5"` — (Optional) Add a description of what the FCIP instance is for. For example, add the description “Access to SAN island 5” to the FCIP instance fcip1.

Assigning an IP Address

To assign an IP address to the FCIP instance:

1. `enable` — Enter Administrator mode.
2. `fcip fcip1 networkif` *`10.1.0.16/24`* — Assign an IP address to the FCIP instance. For example, assign IP address 10.1.0.16 to the FCIP instance fcip1.

   See the *IP Storage Router 2122-2 Command lIne Interface Reference Guide* for more information about the `fcip networkif` command.

Assigning a Peer Name and Peer IP Address

Understanding Flow Control

Connections using the TCP protocol (TCP server or TCP client) rely on TCP to provide adequate flow control. Various FCIP operational parameters are used to configure the receive and transmit window size of the TCP socket.

TCP can configure the number of outstanding FC transmissions, using a counter to limit the number of frames to give to the FC firmware. The TCP protocol acknowledges the data as soon as the FCIP instance reads the data out of the socket, rather than when the data has completed transmission on the FC interface.

Understanding Error Recovery

Connections using the TCP protocol rely on TCP to provide adequate error recovery. There are no FCIP operational parameters available, because TCP does not provide configurable values for retransmit timeouts. The retransmit timeout values that are automatically provided by TCP may or may not be adequate for FCIP frames.

TCP Protocol

Using the TCP protocol, one FCIP instance must be configured as the TCP client; the other FCIP instance must be configured as the TCP server. The only difference between FCIP instances configured as TCP client and TCP server is which FCIP instance initiates the connection; the TCP client initiates the connection.

TCP Client

If the peer FCIP instance is configured as a TCP client, use the following procedure to configure the FCIP instance with the IP address and TCP server protocol of the peer.

1. `enable` — Enter Administrator mode
2. `fcip fcip2 destination tcpserver` *`10.1.0.47`* — Assign the IP address of the peer FCIP instance and configure the protocol.

   For example, the IP address of the peer is in dotted quad notation *10.1.0.47* and connection is made using TCP protocol with fcip2 acting as a TCP server. The TCP server will listen for a TCP connection attempt from its peer which must be configured as a TCP client.

Note: If you are configuring two FCIP instances on the SR2122-2, do not configure both instances as TCP servers. Instead, configure both instances as TCP clients or one as a TCP server and the other as a TCP client. If both instances have to be TCP servers then they should use different TCP ports.

   See the *IP Storage Router 2122-2 Command Line Interface Reference Guide* for more information about the `fcip destination` command.

TCP Server

If the peer FCIP instance is configured as a TCP server, use the following procedure to configure the FCIP instance with the IP address and TCP client protocol of the peer.

1. `enable` — Enter Administrator mode
2. `fcip` *`fcip2`* `destination tcpclient` *`10.1.0.46`* — Assign the IP address of the peer FCIP instance and configure the protocol.

   For example, the IP address of the peer is in dotted quad notation *10.1.0.46* and connection is made using TCP protocol with fcip2 acting as a TCP client. The TCP client will try to initialize the TCP connection with its peer which must be configured as a TCP server.

   See the *IP Storage Router 2122-2 Command Line Interface Reference Guide* for more information about the `fcip destination` command.

Configuring Operational Parameters

For FCIP deployment, a large maximum transfer unit (MTU) size is desirable. To set the size of the MTU, use the `interface ge? mtusize` command to set MTU to its highest level, 9000, if possible.

To configure FCIP operational parameters, use the `fcip destination config` command. The default settings for operational command parameters are listed in this section. If modifications to these settings are necessary, see the *IP Storage Router 2122-2 Command Line Interface Reference Guide* for details about the `fcip destination config` command.

Table 16: Optional Operational Parameters: TCP Protocol

Description	Default	Keyword
Compress the FCIP data stream.	off	**compression**
Batch multiple FC frames in one TCP segment.	yes	**batchtcp**
Maximum number of frames given to the Fibre Channel interface	688	**frinhiwater**
Number of seconds before a keep-alive packet is sent across an idle connection	15	**idlepingdelay**
Value of the packet trace mask. Packets are traced for debugging problems. Range is from 0x0000 to 0xffff. A value of zero will disable packet tracing.	0xffff	**pkttracemask**
Maximum number of outstanding bytes that can be received on a TCP connection	262144	**rxtcpwinsize**
TCP port number where the server is listening to and where the client is connecting to	3225	**tcpport**
Maximum number of outstanding bytes that can be transmitted on a TCP connection	2097152	**txtcpwinsize**
Minimum expected and/or allotted bandwidth in Mbits/sec for this FCIP configuration	0	**pacingRate**

Verifying and Saving Configuration

Verify the FCIP configuration using the procedures that follow. You can save the configuration at any time by using the `save all bootconfig` command. You must save the running configuration to the bootable configuration for it to be retained in the storage router when it is rebooted. Once you have saved the configuration, you can verify that the configuration to be used when the storage router is rebooted matches the currently running configuration.

To verify FCIP configuration:

1. `enable` — Enter Administrator mode.
2. `show fcip` *`fcip1`* — Displays the operational and connection information for FCIP instance fcip1. See Example 10 for a TCP server and Example 11 for a TCP client.

Example 10: Verifying Existence of an FCIP instance for a TCP server

```
[SR2122-2local]# show fcip fcip1
Instance  Device I/F  Network I/F
--------  ----------  -----------
fcip1     fc1         ge1 10.0.0.24

Description
-----------
Access to SAN island 5

Destination   LocalMode  IpAddress        IsConnected
-----------   ---------  ---------------  -----------
fcip          tcpserver  10.0.0.25        TRUE

LinkState
---------
UP

fcip1 Trace Status
------------------
pktTracing                  On, mask 0xffff
mboxTracing                 On
mboxCmdCount                0
```

```
fcip1 Credit Information
------------------------
Receive Credits              61
Transmit Credits           16


fcip1 Connection Information
----------------------------
idlePingDelay                60
Compression:                 Off
tcpPort                      3225
rxTcpWindowSize              262144
maxRxTcpWindowSize           262144
txTcpWindowSize              262144
txTcpCongestionWindowSize    524280
maxTxTcpWindowSize           262144
frIn                         0
frInHiWater                  688
```

Example 11: Verifying Existence of an FCIP instance for a TCP client

```
[SR2122-2remote]# show fcip fcip1
Instance  Device I/F  Network I/F
--------  ----------  -----------
fcip1     fc1        ge1 10.0.0.25

Description
-----------
Access to SAN island 5

Destination   LocalMode  IpAddress        IsConnected
-----------   ---------  ---------------  -----------
fcip          tcpclient  10.0.0.24        TRUE

LinkState
---------
UP
```

```
fcip1 Trace Status
------------------
pktTracing                  On, mask 0xffff
mboxTracing                 On
mboxCmdCount                0

fcip1 Credit Information
------------------------

Receive Credits             61
Transmit Credits          16


fcip1 Connection Information
---------------------------
idlePingDelay               60
Compression:                Off
tcpPort                     3225
rxTcpWindowSize             262144
maxRxTcpWindowSize          262144
txTcpWindowSize             262144
txTcpCongestionWindowSize   524280
maxTxTcpWindowSize          262144
frIn                        0
frInHiWater                 688
```

Configuring Authentication

10

This chapter explains how to configure the authentication portion of HP authentication, authorization, and accounting (AAA) methods on the storage router, and how to enable iSCSI authentication, which uses the AAA authentication methods.

The following tasks are covered:

- Prerequisite Tasks
- Using iSCSI Authentication
- AAA Security Services
- Configuration Tasks
- Configuring Security Services
- Building the AAA Authentication List
- Testing iSCSI Authentication
- Enabling iSCSI Authentication
- Verifying and Saving Configuration

The AAA authentication function is always enabled for the SR 2122-2 Storage Router; it cannot be disabled.

Authentication parameters can be configured using CLI commands, as described in this chapter, or via the web-based GUI. To access the web-based GUI, point your browser to the management interface IP address of the storage router. After logging on, click the Help link to access online help for the GUI.

Prerequisite Tasks

Before performing AAA and iSCSI authentication configuration tasks on the storage router, make sure you have configured system parameters as described in Chapter 5, "Configuring the Storage Router" and Chapter 6, "Configuring System Parameters" If the storage router is deployed for SCSI routing, you should also configure SCSI routing instances as described in Chapter 8, "Configuring SCSI Routing" before proceeding.

Note: AAA and iSCSI authentication configuration settings are system-wide parameters and are not shared across a cluster. However, you may prefer to configure all storage routers in a cluster with the same authentication settings.

Using iSCSI Authentication

iSCSI authentication provides a mechanism to authenticate all IP hosts that request access to storage via a SCSI routing instance. When enabled, iSCSI drivers provide user name and password information each time an iSCSI TCP connection is established. iSCSI authentication uses the iSCSI CHAP (Challenge Handshake Authentication Protocol) authentication method. Authentication services are provided by the AAA subsystem configured for each storage router.

Authentication, authorization and accounting (AAA) is an architectural framework for configuring a set of three independent security functions in a consistent, modular manner. The storage router implements the authentication function.

Authentication provides a method of identifying users (including login and password dialog, challenge and response, and messaging support) prior to receiving access to the requested object, function, or network service. AAA authentication is configured by defining a list of authentication services. iSCSI authentication, which uses the AAA authentication services list, can be enabled for specific SCSI routing instances.

AAA Security Services

iSCSI authentication uses AAA security services to administer its security functions. If you are using remote security servers, AAA is the means through which you establish communications between the storage router and the remote RADIUS or TACACS+ security server.

This chapter describes how to configure the following AAA security services:

- RADIUS is a distributed client/server system implemented through AAA that secures networks against unauthorized access. In this implementation, the storage router sends authentication requests to a central RADIUS server that contains all user authentication and network service access information.
- TACACS+ is a security application implemented through AAA that provides centralized validation of users attempting to gain access to storage targets through specified SCSI routing instances. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. TACACS+ provides for separate and modular authentication, authorization, and accounting facilities.
- Local or local-case uses a local username database on the storage router for authentication. Local-case indicates that the user name authentication is case-sensitive. Password authentication is always case-sensitive.

Configuration Tasks

To configure iSCSI authentication and the associated AAA authentication services on the storage router:

1. Configure the desired security services, such as RADIUS, TACACS+, or the local username database.
2. Build the AAA authentication list.
3. Test the iSCSI authentication services.
4. Enable iSCSI authentication for individual SCSI routing instances.
5. Verify and save AAA and iSCSI authentication configuration.

Figure 50 illustrates AAA authentication configuration elements and Figure 51 illustrates the example configuration of iSCSI authentication and AAA authentication services used in this chapter.

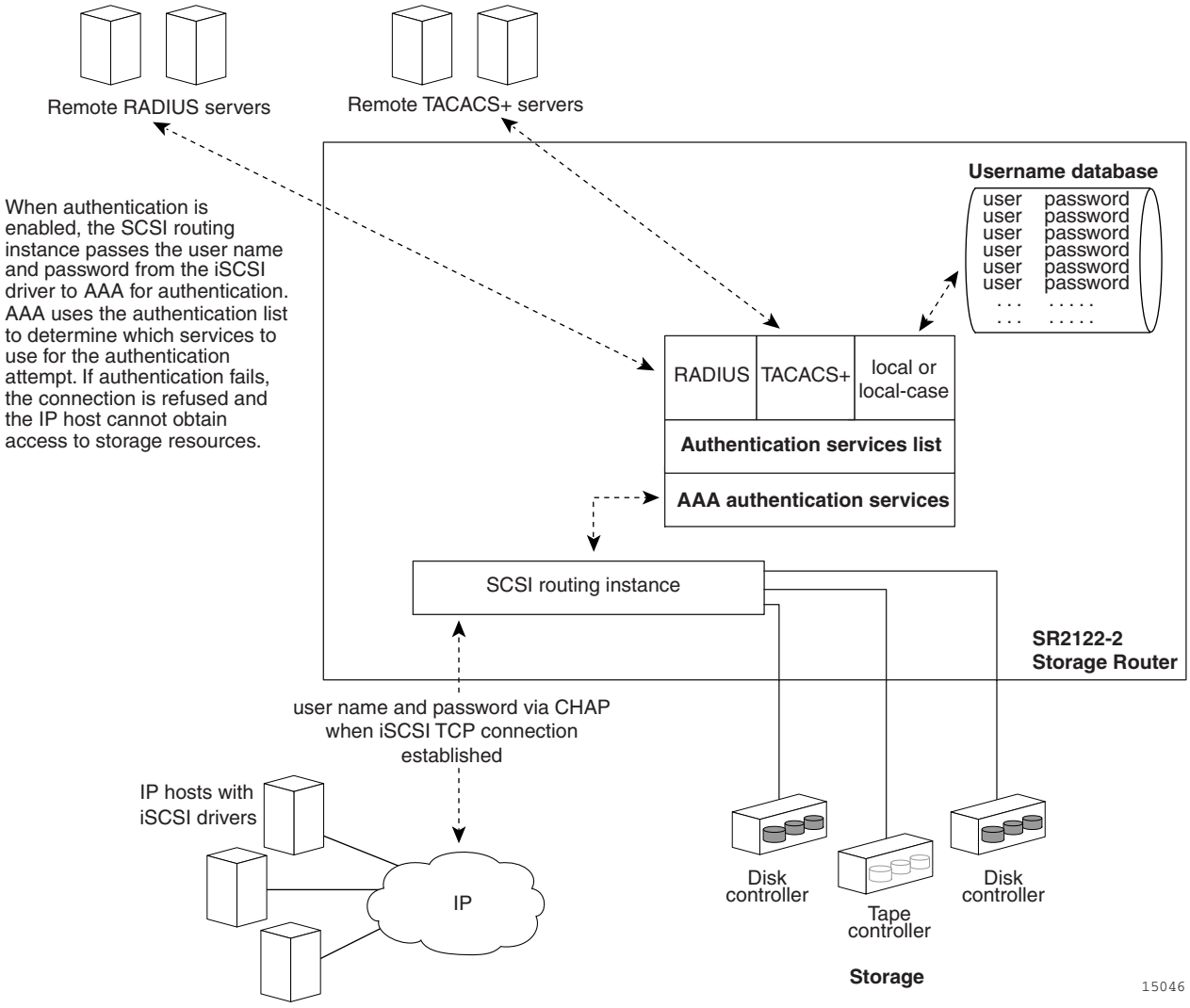


Figure 50: iSCSI authentication configuration elements

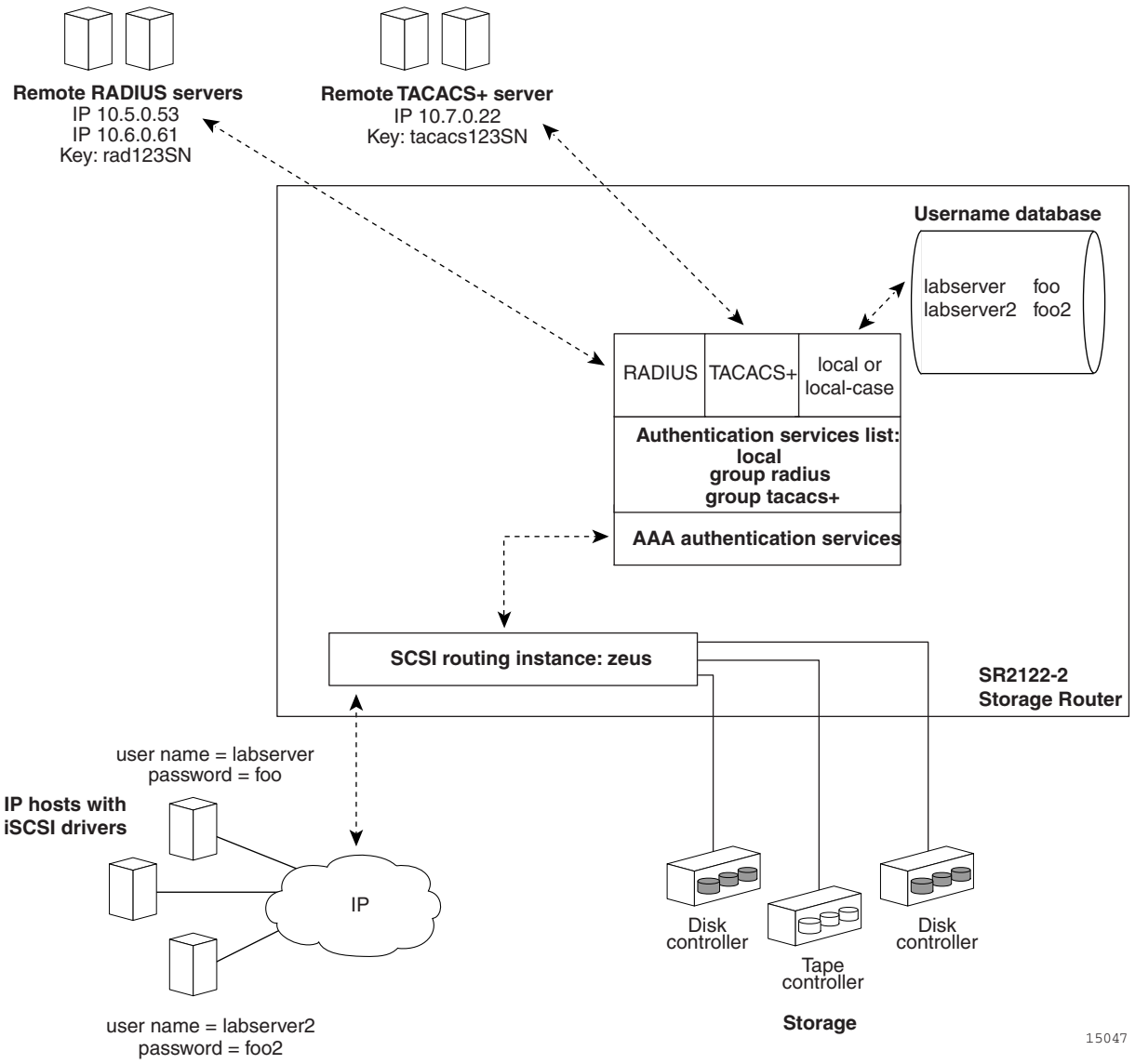


Figure 51: iSCSI authentication example configuration

Configuring Security Services

Configuring security services consists of setting the appropriate parameters for the various service options that can be used by the storage router. The SR2122-2 can use any or all of the supported security services.

Use the procedures that follow to configure the storage router to use the appropriate security services:

- RADIUS Servers
- TACACS+ Hosts
- Local Username Database

RADIUS Servers

To configure RADIUS security services:

1. `enable` — Enter Administrator mode.
2. `radius-server host` *`10.5.0.53`* — Specify the RADIUS server to be used for AAA authentication services. For example, specify the RADIUS server at 10.5.0.53 for use by the storage router. Because no port is specified, the authentication requests use the default UDP port 1645. Global timeout and retransmit values are also used.
3. `radius-server host` *`10.6.0.61`* — Specify a secondary RADIUS server. RADIUS servers are accessed in the order in which they are defined. For example, specify the RADIUS server at 10.6.0.61 as the second RADIUS server to be used for AAA authentication services.
4. `radius-server key` *`rad123SN`* — Configure the global authentication and encryption key to be used for all RADIUS communications between the storage router and the RADIUS daemon. For example, set the key to rad123SN. This key must match the key used on the RADIUS daemon.

TACACS+ Hosts

To configure TACACS+ security services:

1. `enable` — Enter Administrator mode.
2. `tacacs-server host` *`10.7.0.22`* — Specify the TACACS+ server to be used for AAA authentication services. For example, specify the TACACS+ server at 10.7.0.22 for use by the Storage Router. Because no port is specified, the authentication requests use the default port 49. The global timeout value is also used.
3. `tacacs-server key` *`tacacs123SN`* — Configure the global authentication and encryption key to be used for all TACACS+ communications between the storage router and the TACACS+ server. For example, set the key to tacacs123SN. This key must match the key used by the TACACS+ daemon.

Local Username Database

To configure a local username database:

Note: Passwords are entered in clear text but are changed to "XXXXX" in the CLI command history cache and are stored in the local username database in encrypted format.

---

1. `enable` — Enter Administrator mode.
2. `username` *`labserver`* `password foo username` *`labserver2`* `password` *`foo2`* — Enter a user name and password for each device requiring authentication prior to access to storage. For example, add the following user name and password combinations:
   - `labserver and foo`
   - `labserver2 and foo2`

   User name and password pairs must match the user name and password pairs configured for the iSCSI drivers that require access to storage via the SCSI routing instances that have iSCSI authentication enabled. If other authentication services are also used (such as RADIUS or TACACS+), these user name and password pairs must also be configured within the databases those services use for authentication purposes.

The following rules apply to passwords:

- Passwords are entered in clear text. However, they are stored in an encrypted format.
- If the password contains embedded spaces, enclose it with single or double quotes.
- After initial entry, passwords display in their encrypted format. Use the `show aaa` command to display the local username database entries. The following is an example display:

```
username "foo" password
"9 ea9bb0c57ca4806d3555f3f78a4204177a"
```

Note: The first "*9*" in the example display indicates that the password is encrypted.

- You can re-enter an encrypted password using the normal `username password` command. Enter the encrypted password in single or double quotes, starting with 9 and a single space. For example, copying and pasting password `"9 ea9bb0c57ca4806d3555f3f78a4204177a"` from the example above into the `username pat` command would create an entry for `pat` in the username database. The user named `pat` would have the same password as the user named `foo`. This functionality allows user names and passwords to be restored from saved configuration files.
- When entering a password, a zero followed by a single space indicates that the following string is not encrypted; 9 followed by a single space indicates that the following string is encrypted. To enter a password that starts with 9 or zero, followed by one or more spaces, enter a zero and a space and then enter the password string. For example, to enter the password "`0 123`" for the user named `pat`, enter this command:

```
username pat password "0 0 123"
```

```
To enter the password "9 73Zjm 5" for user name
lab1, use this command:
```

```
username lab1 password "0 9 73Zjm 5"
```

Building the AAA Authentication List

iSCSI authentication uses a list of defined AAA authentication services to administer its security functions. The list that is created must be named *default*.

To build a list of AAA authentication services to be used for iSCSI authentication:

1. `enable` — Enter Administrator mode.
2. `aaa authentication iscsi` *`default`* `local group radius group tacacs+` — Create a list (named default) of authentication services. For example, build a list so that AAA first tries to perform authentication using the local username database. If AAA fails to find a user name match, an attempt is made to contact a RADIUS server. If no RADIUS server is found, RADIUS returns an error and AAA tries to use a TACACS+ server. If no TACACS+ server is found, TACACS+ returns an error and AAA authentication fails. If a RADIUS or TACACS+ server does not find a user name and password match, authentication fails and no other methods are attempted.

Note: If local or local-case is the first service in the authentication list and a user name match is not found, the next service in the list will be tried. If local or local-case is not the first service, authentication fails if a user name match is not found. Authentication always fails if a RADIUS or TACACS+ server fails to find a user name match.

Testing iSCSI Authentication

Before enabling iSCSI authentication for a SCSI routing instance, you can test iSCSI authentication from the storage router. The user name and password are passed to AAA authentication, which performs authentication using the iSCSI default authentication list. The command response indicates a pass or fail status.

To test iSCSI authentication:

1. `enable` — Enter Administrator mode.
2. `aaa test authentication iscsi default` *`labserver foo`* and `aaa test authentication iscsi default` *`labserver2 foo2`* — Test the user names and passwords listed in the username database. AAA authentication uses the services in the default list for authentication.

Example 12: Testing Authentication

```
*[SR2122-2-MG1]# aaa test authentication iscsi default labserver foo


Sep 02 14:37:00:aaa:AS_NOTICE :Auth test request being
queued


Sep 02 14:37:00:aaa:AS_NOTICE :Auth test request complete,
status = pass
```

Enabling iSCSI Authentication

iSCSI authentication is enabled for specific SCSI routing instances. By default, iSCSI authentication is not enabled.

To enable iSCSI authentication using the AAA authentication methods configured in the default AAA authentication list:

1. `enable` — Enter Administrator mode.
2. `scsirouter` *`zeus`* `authenticate` *`yes`* — Enable authentication for the named SCSI routing instance. For example, enable authentication for the SCSI routing instances named zeus.

Verifying and Saving Configuration

You can save the configuration at any time using either the `save aaa bootconfig` or `save all bootconfig` commands. You must save the authentication configuration for it to be retained in the storage router when it is rebooted.

To verify and save authentication settings:

1. `enable` — Enter Administrator mode.
2. `show aaa` — Display AAA authentication configuration (Example 13).
3. `show scsirouter` *`zeus`* — Verify that iSCSI authentication is enabled for SCSI routing instances **zeus** (Example 14).
4. `save aaa bootconfig` — Save authentication settings.
5. `save scsirouter` *`zeus`* `bootconfig` — Save the SCSI routing instances.
6. `save all bootconfig` — Save all configuration settings. This command may be used in place of individual `save aaa bootconfig` and `save scsirouter bootconfig` commands described in Steps 4 and 5 (Optional).

Example 13: Display AAA Authentication Configuration

```
[SR2122-MG1]# show aaa
aaa new-model
aaa authentication iscsi default local group radius group
tacacs+
username "LabServer" password
"9 3b7e1560943b2c3df73ae16dd8c21406ad"
username "LabServer2" password
"9 5a034dba7085f7628852db4637787b3f9e"
radius-server key "9 4f5e3deda858731566fa8c7fa23d8a5b4d"
radius-server timeout 100
radius-server retransmit 3
radius-server host 10.5.0.53 auth-port 1645
radius-server host 10.6.0.61 auth-port 1645
tacacs-server key "9 10d2a453d607e75f36ca96dfc5d36b4495"
tacacs-server host 10.7.0.22 auth-port 49
```

Example 14: Verify iSCSI Authentication for SCSI Routing Instance

```
[SR2122-MG1]# show scsirouter zeus
zeus description "(not set)"
zeus authentication "yes"
zeus primary "none"
zeus target naming authority "none"
zeus serverif ge2 10.1.0.45/24
zeus target chimaera_apps description "(not set)"
zeus target chimaera_apps WWUI
"iqn.1987-05.com.hp.00.0b1aaa415a4146aa2d899c47070c3c06.chim
aera_apps"
zeus target chimaera_apps enabled "TRUE"
zeus target chimaera_apps accesslist "none"
zeus target chimaera_apps lun 24 wwpn
"22:00:00:20:37:19:15:05" lun "0"
zeus target chimaera_eng description "(not set)"
zeus target chimaera_eng WWUI
"iqn.1987-05.com.hp.00.0b1aaa415a4146ab2d799c45070c3d06.chim
aera_eng"
zeus target chimaera_eng enabled "TRUE"
zeus target chimaera_eng accesslist "aegis"
zeus target chimaera_eng lun 17 wwnn
"22:00:00:20:37:19:12:9d"
zeus target pegasus_email description "(not set)"
zeus target pegasus_email WWUI
"iqn.1987-05.com.hp.00.0b1aca415a6146ea2d809c44070c2c06.pega
sus_email"
zeus target pegasus_email enabled "TRUE"
zeus target pegasus_email accesslist "all"
zeus target pegasus_email wwpn "22:00:00:20:37:19:12:da"
```

Configuring a High Availability Cluster

11

This chapter explains how to configure SR2122-2 Storage Routers in a cluster to allow the storage routers to back each other up in case of failure. The following tasks are covered:

- Prerequisite Tasks
- Adding the Storage Router to a Cluster
- Changing Clusters

High availability clusters can be configured using CLI commands, as described in this chapter, or via the web-based GUI. To access the web-based GUI, point your browser to the storage router management interface IP address. After logging on, click the Help link to access online help for the GUI.

Prerequisite Tasks

Before performing any high availability cluster configuration tasks, make sure you have configured system parameters, including the HA interface, as described in Chapter 5, "Configuring the Storage Router" and Chapter 6, "Configuring System Parameters"

When you configure SCSI routing instances to run in a high availability cluster, follow these guidelines:

- If you map targets using WWPN, be sure to specify both the primary WWPN (the WWPN associated with the storage resource as known to the primary storage router in the cluster) and the secondary WWPN (the WWPN associated with the storage resource as known to the second storage router in the cluster).
- Automatic failover of a SCSI routing instance occurs if the Gigabit Ethernet interface is unavailable or if all mapped targets are unavailable. If some targets are available and others are not, the SCSI routing instance will not automatically fail over. All SCSI routing instances will failover if the storage router running the instances fails to exchange heartbeats within the high availability cluster.

  To maximize the potential for automatic failover in case of target unavailability, map the targets associated with a single SCSI routing instance to storage that is available through one Fibre Channel interface. Do not map the targets associated with a single SCSI routing instance to storage that is available through multiple FC interfaces.

  This type of mapping minimizes the potential for a mixed target availability condition, which prevents IP hosts from accessing some storage but does not cause an automatic failover of the SCSI routing instance.

Adding the Storage Router to a Cluster

In most situations, you will completely configure a principal storage router (including all cluster-wide settings), and then add a new, unconfigured storage router or a minimally configured storage router to the cluster. A high availability cluster is composed of two storage routers.

The following storage router configuration settings are shared cluster-wide, and when configured on the first storage router in the cluster, will be shared with the other storage router that joins the cluster.

- Access lists
- Cluster name
- SCSI routing instances
- VLAN information (VID, VTP mode, domain name, and so on)

Note: A minimally configured storage router is one in which the management IP address, system name, and optional network management interfaces have been configured. Other system information, such as HA IP address, administrator and monitor passwords, may also have been configured. A minimally configured storage router, however, must not have had any cluster-wide settings configured.

Adding an Unconfigured Storage Router

To add a new, unconfigured storage router to an existing cluster:

1. Respond to the prompts from the storage router initial system configuration script. This script configures the following settings:
   - Management IP address
   - System name
   - HA configuration mode
   - Cluster name
   - HA IP address

   When prompted to select HA configuration mode, choose clustered. When prompted for cluster name, enter the name of the existing cluster. At the end of the initial system configuration script, the storage router automatically reboots.
2. When the storage router restarts, it communicates with the other member of the cluster to obtain current cluster configuration information. Once the storage router is completely restarted, verify the new cluster configuration. Issue the `show cluster` command to verify the cluster name and confirm that the storage router is exchanging heartbeats with the other member of the cluster.

3. To verify that both storage routers in the cluster include the same configuration, issue the following commands from the principal storage router in the cluster:
   - `show accesslist all from bootconfig`
   - `show scsirouter all from bootconfig`
   - `show vlan`
   - `show vtp`

   Issue the same commands from the storage router just added to the cluster. The displays should be the same.
4. Use the Setup Configuration Wizard, CLI commands, or the GUI to complete storage router configuration. See Chapter 5, "Configuring the Storage Router" and Chapter 6, "Configuring System Parameters" for complete details.
5. Save any changes made to the configuration by issuing the appropriate `save` command with the bootconfig keyword, which updates the bootable configuration for the storage router and notifies all storage routers in the cluster of the configuration changes. (Optional)
6. To divide the workload between the storage routers in the cluster, you can manually failover selected SCSI routing instances using the `failover scsirouter` command. For additional information about failing over SCSI routing instances, refer to Chapter 8, "Creating a SCSI Routing Instance" (Optional).

Adding a Minimally Configured Storage Router

To add a minimally configured storage router to an existing cluster, perform the following steps:

1. Run the Setup Cluster Configuration Wizard:
   - When prompted to select HA configuration mode, choose clustered.
   - When prompted for cluster name, enter the name of the existing cluster.
   - When prompted to retain or delete scsirouter instances, enter delete. Deleting means that any existing SCSI routing instances will be deleted from this storage router.
   - Enter yes to confirm your changes. The storage router automatically reboots.

2. When the storage router restarts, it communicates with other member of the cluster to obtain current cluster configuration information. Once the storage router is completely restarted, verify the new cluster configuration. Issue the `show cluster` command to verify the cluster name and confirm that the storage router is exchanging heartbeats with the other member of the cluster.
3. To verify that both storage routers in the cluster include the same configuration, issue the following commands from the principal storage router in the cluster:
   - `show accesslist all from bootconfig`
   - `show scsirouter all from bootconfig`
   - `show vlan`
   - `show vtp`

   Issue the same commands from the storage router just added to the cluster. The displays should be the same.
4. Complete additional system configuration of the storage router just added to the cluster, as needed. For example:
   - Use the **Setup Access Configuration** Wizard to configure passwords for the storage router.
   - Use the **Setup Netmgmt Configuration** Wizard to configure the storage router for network management via SNMP.
   - Use the **Setup Time Configuration** Wizard to configure the storage router date and time, and optional NTP server information.
   - Use the CLI or GUI to configure AAA authentication. See Chapter 10, "Configuring Authentication" for additional information.
5. Save any changes to the configuration by issuing the appropriate `save` command with the **bootconfig** keyword, which updates the bootable configuration for the storage router and notifies all storage routers in the cluster of the configuration changes.
6. To divide the workload between the storage routers in the cluster, you can manually failover selected SCSI routing instances using the `failover scsirouter` command. For additional information about failing over SCSI routing instances, refer to "Controlling SCSI Routing Instances in a Cluster" on page 187 and Chapter 12, "Maintaining and Managing the Storage Router" (Optional)

Adding Completely Configured Storage Routers

You may prefer to completely configure both storage routers (including SCSI routing instances and access lists) as standalone systems before joining them into a cluster.

The following example explains the steps required to create a cluster named ***Cluster1***, composed of two storage routers named ***StorageRouterSys1*** and ***StorageRouterSys2.*** This example assumes that both storage routers are fully configured with SCSI routing instances and access lists. (See Chapter 8, "Configuring SCSI Routing" for details.) Use the `scsirouter primary` command to assign a preferred storage router to any or all of the SCSI routing instances, if desired.

Note: A cluster supports up to 12 active SCSI routing instances.

To create a cluster from fully configured storage routers:

1. Use the **setup cluster configuration** wizard to define ***StorageRouterSys1*** as a member of the cluster ***Cluster1***. When prompted, enter retain to keep the access list and SCSI routing instance information already defined.
2. Use the `show cluster` command to verify the cluster name after ***StorageRouterSys1*** reboots. Verify that all instances and access lists are still available, using `show scsirouter` and `show accesslist` commands.
3. On ***StorageRouterSys2***, save any access list information that you want to make available in the cluster to a file, using the `save accesslist` command. (Optional)

   For example, to save all access lists to a file named *StorageRouterSys2_AccessLists.xml*:

```
save accesslist all SR2122Sys2_AccessLists.xml
```

4. Because access lists can only be manipulated from the first storage router in a cluster, the saved configuration file from ***StorageRouterSys2*** must be made available to ***StorageRouterSys1***. See Chapter 12, "Maintaining and Managing the Storage Router" for information on managing storage router saved configuration files using either the `copy savedconfig` command or `FTP`. (Optional)

5. Add ***SvSys2*** to the new cluster named ***Cluster1***, using the **Setup Cluster Configuration** Wizard. When prompted, enter retain to share the existing SCSI routing instances across the cluster.
6. Use the `show cluster` command to verify the cluster name after ***StorageRouterSys2*** reboots. Verify that the defined SCSI routing instances were retained, using `show scsirouter` command.
7. Restore any access lists saved in Step 3 using the `restore accesslist from` command. Access lists can only be manipulated from the first storage router in a cluster, so these commands must be issued from the system ***StorageRouterSys1***. (Optional)
8. Save all configuration information on system ***StorageRouterSys1*** by issuing a `save all bootconfig` command, which updates the bootable configuration of all storage routers in the cluster. (Optional)
9. Verify that all SCSI routing instances are active using the `show scsirouter stats` command on both storage routers.

Changing Clusters

In some situations, you may need to move the storage router from one cluster to another cluster. Moving a fully configured storage router from one cluster to another is more complex than simply adding the storage router to a cluster. Advanced planning is required.

To successfully move the storage router from one cluster to another:

1. Verify that the storage router to be moved has the same hardware configuration as the other storage routers in the cluster you are planning to join. Each storage router in the cluster must have connectivity to the same IP hosts and Fibre Channel storage. All management interfaces for the storage routers within a cluster must be on the same IP subnet, and all HA interfaces for the storage routers within a cluster must be on the same IP subnet. However, the management interfaces must be on a different IP network than the HA interfaces.
2. Decide if you need to retain any SCSI routing instances defined on the storage router joining the cluster. Retaining data means all SCSI routing instances existing on the storage router joining the cluster will be added to those already defined for the cluster. If the existing instances are not retained, they are deleted.

3. If you are going to retain data, determine if you have any duplicate SCSI routing instance names. When the storage router is added to the cluster, the data in the cluster will overwrite the existing data. You may prefer to change the configuration in the storage router before it joins the cluster to prevent this situation.
4. If you are going to retain data, determine if you need to save existing access list information. Access lists are not retained. Any access lists on the storage router will be discarded when it joins the new cluster. You can save the access list information and then restore it to the cluster. Access list information can be restored before or after the storage router joins the cluster by transferring the saved configuration file to the first storage router in the cluster and performing the restore.
5. Use the **Setup Cluster Configuration** Wizard to join the new cluster. Respond to the prompts to retain or delete configuration as required. The storage router will automatically reboot at the end of the configuration wizard.
6. Perform any additional configuration that may be needed. You can fail over SCSI routing instances to this new cluster member to balance traffic load between all storage routers in the cluster.
7. Use the `save all` command with the **bootconfig** keyword to copy and save the storage router configuration, thereby updating the cluster.

Maintaining and Managing the Storage Router

12

This chapter explains how to perform normal maintenance and management tasks associated with the storage router. The following tasks are covered:

- Prerequisite Tasks
- Installing Updated Software
- Backing Up System Configuration
- Restoring from Backups
- Powering Down the Storage Router
- Resetting the System
- Recovering Passwords
- Controlling SCSI Routing Instances in a Cluster
- Managing CDP on the storage router
- Using Scripts to Automate Tasks
- Managing the Log File
- Gathering Troubleshooting Information

Storage router maintenance and management tasks can be performed using CLI commands as described in this chapter or via the web-based GUI. To access the web-based GUI, point your browser to the storage router management interface IP address. After logging on, click the Help link to access online help for the GUI.

Note: Not all maintenance and management tasks are appropriate for all storage routers. For example, tasks related to high availability clusters (such as failover of SCSI routing instances) are not necessary for storage routers configured as standalone systems.

Prerequisite Tasks

Before performing any storage router maintenance tasks, make sure you have configured system parameters as described in Chapter 5, "Configuring the Storage Router" and Chapter 6, "Configuring System Parameters".

Note: Certain configuration tasks, such as identifying a location from which to download software, are optional and may not have been performed during initial configuration. You may perform these tasks at any time, via the CLI or the GUI. Where necessary, this chapter will identify the relevant tasks and commands.

Installing Updated Software

The storage router is designed to run on a continual basis without significant maintenance. However, from time to time, you may need to install updated software. The storage router stores software images (along with configuration files, log files, and other information) on a local file system. This file system is stored on an internal, non-volatile Flash disk. The `show software version all` command displays a list of all software versions stored on the storage router and the amount of disk space available for additional software.

http://www.hp.com/support provides registered users access to storage router software updates. You can download updated software directly to the storage router from HP.com via standard HTTP, or via HTTP using a proxy server. You can also use a standard browser to download software updates and associated readme files from http://www.hp.com/support to a location of your choosing. Using the CLI or the web-based GUI, you can then make software available from this location (known as the "download location") to the Store Router via HTTP, HTTP using a proxy server, or Trivial File Transport Protocol (TFTP).

Note: Always review the readme file before making updated software available to the storage router.

If you plan to use the CLI `download software http` or `download software proxy` commands to make the updated software available to the storage router, the machine hosting the download location must be running a web server. If you plan to use the CLI `download software tftp`

command, the machine must be accessible using the Trivial File Transport Protocol. If the machine is not running a web server or accessible via TFTP, use the storage router web-based GUI to make the updated software available to the storage router. (See the online Help for details.)

The download location used for retrieving updated storage router software is set using the `software http url`, `software proxy url`, or the `software tftp` commands. To view the download location currently specified, use the `show software version all` command (Example 15). The `show software version all` command identifies the HTTP URL, Proxy URL, and TFTP host name and other information used to identify the download location, the current version of software running on the storage router, and the version that will be used at system restart. In the example, all default locations and related user names and passwords are set.

Note: If you are a registered HP.com user, you can download a TFTP server tool for Microsoft Windows 95, Microsoft Windows 98, and Microsoft Windows NT. You can reach the TFTP server tool on HP.com at the Software Center under Service & Support: http://www.hp.com/support.

Example 15: Results of "show software version all" Command

```
[SR2122-2_A01]# show software version all
Version    Boot  Hash  Sign  Crash  Size     Date
---------  ----  ----  ----  -----  -----    ----------
2.3.0.49   OK    OK    N/A   0      18585600 Mar 21 18:08
CST 2002
2.3.1      OK    OK    N/A   0      18616320 Mar 22 16:35
CST 2002



Http Url: http://www.HP.com
Http Username: SWAdmin01
Http Password: *********



Proxy Address: 10.1.12.32
Proxy Port: 3122
```

```
Proxy Url: http://www.hp.com
Proxy Username: SWAdmin01
Proxy Password: *********


Tftp Hostname: 10.1.1.122
Tftp Directory: SR2122/v2.3/


Disk Space Available: 13357.0 KB
Current Version: 2.3.1
Boot Version: 2.3.1
```

To update storage router software:

1. Identify the location from which to retrieve the updated storage router software. (This is either http://www.hp.com/support or another download location of your choosing, as previously described.) (Optional)
2. Make the selected version of software available on the storage router local file system.
3. Set the new version as the version to be booted during the next system restart, and reboot the storage router. (Optional)

Specifying the Location to Retrieve Updated Software

You must specify the location from which to retrieve updated software. If the current download location is not appropriate, you can reset it. To specify the desired download location:

- Using HTTP
- Using Proxy Services
- Using TFTP

When you are finished, verify the new settings using the `show software version all` command, then save them using the `save system bootconfig` or `save all bootconfig` command.

Using HTTP

To specify the HTTP download location:

1. `enable` — Enter Administrator mode.
2. `show software version all` — List the software versions currently available for booting, along with the current download locations. Verify that the version of software required is not already available. Verify that the current download location information for HTTP is correct.
3. `software http url http://10.1.11.32/~software/SR2122-2` — If the current download location is not the one from which you would normally retrieve updated software, reset the current download location. For example, reset your current download location to http://10.1.11.32/~software/SR2122-2. (Optional)
4. `software http username webadmin password webword` — Use this command to define the user name and password needed to access the selected location. For example, specify user name webadmin and password webword. If no user name and password are required, use the keyword none (for example, `software http username none`). (Optional)

Note: If you are using the default URL, http://www.hp.com, the username and password must be the same as your hp.com login ID and password.

Using Proxy Services

To specify a download location via proxy services:

1. `enable` — Enter Administrator mode.
2. `show software version all` — List the software versions currently available for booting, along with the current download locations. Verify that the version of software required is not already available. Verify that the current download location information for HTTP via proxy server is correct.
3. `software proxy url default` — If the current download location is not the one from which you would normally retrieve updated software, reset the current download location. For example, reset your current download location to the **default** (http://www.hp.com). (Optional)

4. `software proxy address` *`http://10.1.10.126`* `port` *`32`* — This is the address and port number of the proxy server that will be used to access the URL specified in Step 3 (for example, http://10.1.10.126, port 32). (Optional)
5. `software proxy username` *`HPuser`* `password` *`HPpswd`* — Use this command to define the user name and password needed to access the selected download location. For example, specify user name HPuser and password HPpswd. If no user name and password are required, use the keyword none (for example, `software proxy username none`). (Optional)

Note: If you are using the default URL, http://www.hp.com, the username and password must be the same as your hp.com login ID and password.

Using TFTP

To specify the TFTP download location:

1. `enable` — Enter Administrator mode.
2. `show software version all` — List the software versions currently available for booting, along with the current download locations. Verify that the version of software required is not already available. Verify that the current download location information for TFTP is correct.
3. `software tftp hostname` *`TFTPHost1`* `directory` */tftpboot* — If the current host name and base directory location are not the ones from which you would normally retrieve updated software, reset the host and optional base directory. For example, set the host name to TFTPHost1 and the base directory to `/tftpboot`. If a DNS is not defined for the storage router, enter the IP address of the TFTP host.

Downloading Updated Software

The `download software` command makes a new version of software available to the storage router for boot purposes. You can store two versions of software on the storage router. Before attempting to download updated software, verify that only a single version of software exists on the storage router.

To make a new version of software available to the storage router:

- Using HTTP
- Using Proxy Services
- Using TFTP

Using HTTP

To make a new version of software available to the storage router via HTTP:

1. `enable` — Enter Administrator mode.
2. `show software version` *`all`* — Verify that there is only one version of software on the storage router. If two versions exist, use the `delete software version` command to delete the old version of software to make room for the new version.
3. `download software http version` *`3.1.3`* — Download a new software version to the storage router (for example, 3.1.3).

Note: There may be times when you need to make special software available to the storage router, for example, under the guidance of a HP Technical Support professional. If you isolate this software from standard updates by placing it in another location (not the default download location), you could change the default download location, download the software, and then reset the default download location. An easier way, however, is to specify the download location via the URL parameter on the `download software http` command. For example, to download a file named **313.tar** containing version 3.1.3 software from `http://your.website.com/StorageRouter`, issue this command: `download software http url http://your.website.com/StorageRouter/313.tar`.

Using Proxy Services

To make a new version of software available to the storage router via proxy services:

1. `enable` — Enter Administrator mode.
2. `show software version` *`all`* — Verify that there is only one version of software on the storage router. If two versions exist, use the `delete software version` command to delete the old version of software to make room for the new version.
3. `download software proxy version` *`3.1.3`* — Make a new software version available to the storage router (for example, **3.1.3**).

Note: There may be times when you need to make special software available to the storage router, for example, under the guidance of a HP Technical Support professional. If you isolate this software from standard updates by placing it in another location (not the default download location), you could change the default download location, download the software, and then reset the default download location. An easier way, however, is to specify the download location via the URL parameter on the `download software proxy` command. For example, to download a file named **313.tar** containing version 3.1.3 software from `http://your.website.com/StorageRouter` using the services of a proxy server, issue this command:
`download software proxy url http://your.website.com/StorageRouter/313.tar`.

Using TFTP

To make a new version of software available to the storage router via TFTP:

1. `enable` — Enter Administrator mode.
2. `show software version all` — Verify that there is only one version of software on the storage router. If two versions exist, use the `delete software version` command to delete the old version of software to make room for the new version.
3. `download software tftp version 3.1.3` — Make a new software version available to the storage router (for example, **3.1.3**).

Note: There may be times when you need to make special software available to the storage router, for example, under the guidance of a HP Technical Support professional. If you isolate this software from standard updates by placing it in another location (not the default download location), you could change the default download location, download the software, and then reset the default download location. An easier way, however, is to specify the download location via the hostname and filename parameters on the `download software tftp` command. For example, to download a file named ***313.tar*** containing version 3.1.3 software from my_tftpHost using TFTP, issue this command:
`download software tftp hostname my_tftp Host` filename **313.tar**. The **313.tar** file must reside in the default base directory defined for the TFTP host.

Setting Updated Software as Boot Version

Downloading updated software to the storage router does not change the currently running version of the software, nor does it automatically set the new version to be booted at next system restart. You must take specific action to make the new software version bootable.

Setting software as the bootable version consists of verifying the software integrity and performing internal checks to ensure that the storage router can boot the specified version of software.

To set the new software as the version to be booted:

1. `enable` — Enter Administrator mode.
2. `software version` *`3.1.3`* — Select the software to be booted when the system next starts (for example, boot **3.1.3** when the system restarts). The system checks the integrity of the specified software version to be sure that it is bootable.
3. `show software version boot` — Verify that the correct version is shown as the bootable version (identified as Boot Version).
4. `reboot` — Restart the storage router to run the new software. (Optional)

When you set a new software version as the bootable version, internal checks are made to ensure that the new software can be run.

Precautions for Cluster Environments

In a cluster environment, the `software version` command may temporarily suspend normal HA communications, while internal checks are made to ensure that the new software can be run. A suspension will cause a failover of any SCSI routing instances active on the storage router.

Any instances with the primary attribute set to the name of the storage router will resume running on the storage router after it is rebooted. If you are not going to reboot the storage router immediately, use the `failover scsirouter` command to return the desired SCSI routing instances to the storage router.

If the storage router is running in a cluster environment, issuing the `reboot` command will attempt failover for all SCSI routing instances to another storage router in the cluster. The iSCSI drivers handle reconnection of users to the appropriate storage resources, minimizing the effects of the reboot sequence on those users.

Backing Up System Configuration

Backing up the system configuration consists of saving selected storage router configuration information to XML files that can be stored both locally and remotely. Should problems occur, AAA authentication information, SCSI routing instances, access lists, VLANs, and other storage router system configuration information can be restored from these files.

While you can issue a `save` command at any time during a CLI command session, best practices suggest that you should back up the storage router system configuration to a file on a regular basis.

Configuration files are normally maintained in the `savedconfig` directory on the storage router. You can use the `copy` command to copy the configuration file to a server running TFTP, allowing you to integrate the storage router backups with other software archives. By accessing the web-based GUI from a remote server, you can create storage router backup files directly on that server. See the GUI online help for details.

Creating Local Backups

Local backups allow you to store the resulting XML configuration file in the `savedconfig` directory on the storage router.

To perform a local backup that saves the configuration of all the current SCSI routing instances to a file named *backup1* in the `savedconfig` directory:

1. `enable` — Enter Administrator mode.
2. `save scsirouter all` *`backup1`* — Save all defined SCSI routing instances to a file named *backup1*.

Storing Backups to a Remote TFTP Server

To create a backup configuration file named *backup1* and to copy that backup file to another file named *back1.xml*, located on the TFTP host, tftpserver1, in the default directory, `/tftpboot`:

1. `enable` — Enter Administrator mode.
2. `save all` *`backup1`* — Save the current running configuration to a file called *backup1* in the `savedconfig` directory.
3. `copy savedconfig:` *`backup1 tftp://tserver1/back1.xml`* — Copy the saved configuration file, *backup1*, to a file called *back1.xml*, located on the TFTP server, `tserver1`, in the default directory.

Note: The back1.xml file must already exist in the `default` directory with the appropriate permissions that allow it to be overwritten. You cannot create a new file using TFTP.

Restoring from Backups

AAA authentication information, SCSI routing instances, access lists, VLANs, and selected system configuration data can be restored from previously saved configuration files. You may choose to restore selected data such as a specific SCSI routing instance, or all data, using the `restore` command with the `from` keyword.

The file from which configuration is restored must reside in the `savedconfig` directory (`/ata3/savedconfig`). If you need to restore configuration data from a backup file existing elsewhere in the network, use the `copy` command to make the desired file available in the `savedconfig` directory.

Restoring configuration data copies all or part of the contents of the specified file into persistent memory; it does not always change the storage router's running configuration. For example, the configuration of a restored SCSI routing instance may only be completely visible via the `show scsirouter` command using the `from bootconfig` keywords, until the instance has been restarted.

Restoring a Deleted SCSI Routing Instance

For example, suppose the SCSI routing instance, scsi1, was inadvertently deleted. To restore scsi1 from a configuration file that was saved to a URL:

1. `enable` — Enter Administrator mode.
2. `copy` *`http://10.1.1.44/~s1/back1.xml`* `savedconfig:` *`scsi1_restore.xml`* — Copy the specified configuration file from the designated URL and place it in the `savedconfig` directory, using the file name, *scsi1_restore.xml*.
3. `show savedconfig` — Verify that the imported file now exists in the `savedconfig` directory.
4. `show scsirouter all from` *`scsi1_restore.xml`* — Restores SCSI routing instance, scsi1, from the specified file.
5. `show scsirouter` *`scsi1`* `from` *`bootconfig`* — Display the restored SCSI routing instance, scsi1, to verify configuration is as expected.
6. `scsirouter` *`scsi1`* `enable` — Start the restored SCSI routing instance, updating the running configuration of the storage router. Once the instance has been restored and restarted, modifications to its configuration can also be made.
7. `save scsirouter` *`scsi1`* `bootconfig` — If changes are made to the SCSI routing instance configuration, save the SCSI routing instance to the storage router bootable configuration. (Optional)

Restoring an Existing SCSI Routing Instance

If you need to restore the configuration of a SCSI routing instance that is still active in the storage router, you must stop the instance, restore the configuration from the selected file, then restart the instance. For example, to restore the SCSI routing instance, scsi2, from the file, *scsi2_backup*.

1. `enable` — Enter Administrator mode.
2. `show scsirouter` *`scsi2`* `stats` — Display current status of the SCSCI routing instance, scsi2. If the status is active, issue the `no scsirouter enable` command shown in Step 3 to stop the instance.
3. `no scsirouter` *`scsi2`* `enable` — Disable an active SCSI routing instance. You cannot restore an active instance.
4. `show savedconfig` — Confirm that the desired backup file exists in the `savedconfig` directory.
5. `show scsirouter` *`all`* `from` *`scsi2_backup`* — Verify that the instance saved in the configuration file is the one you want to restore.
6. `restore scsirouter` *`scsi2`* `from` *`scsi2_backup`* — Restore the SCSI routing instance.
7. `show scsirouter` *`scsi2`* `from` *`bootconfig`* — Confirm that the configuration of the SCSI routing instance is now correct.
8. `scsirouter` *`scsi2`* `enable` — Restart the SCSI routing instance.
9. `show scsirouter` *`scsi2`* — Verify the configuration of the restored and restarted SCSI routing instance. The running configuration should now match the restored permanent configuration. Once the instance has been restored and restarted, modifications to its configuration can also be made.
10. `save scsirouter` *`scsi2`* `bootconfig` — If changes are made to the SCSI routing instance configuration, save the restored SCSI routing instance to the storage router's bootable configuration.

Restoring an Access List

When you restore an access list, existing entries are never deleted. The restore will add missing entries and overwrite entries of the same name, but will never purge or delete existing entries. If necessary, you can delete an entire access list and then restore if from a saved configuration file.

Use the following procedure to restore the access list, mylist1, from the file, *accesslist_backup.xml*. In this example, mylist1 in the running configuration contains the following entries:

- 10.1.1.30/32
- 172.16.255.220/32
- chap-username 12h7b.lab2.webservices
- chap-username 12784.lab1.webservices

The saved access list in the configuration file, *accesslist_backup.xml*, contains these entries:

- 209.165.200.225/32
- 10.1.1.30/32
- chap-username 12h7b.lab2.webservices
- chap-username test2.sys3

Note: In a cluster environment, access lists management functions are handled by a single storage router. If you issue an `access list` command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the storage router that is currently handling those functions.

---

1. `enable` — Enter Administrator mode.
2. `show accesslist` *`mylist1`* — Display the current entries associated with access list, mylist1.
3. `show accesslist` *`mylist1`* `from` *`accesslist_backup.xml`* — Display the entries associated with access list, mylist1, saved in the configuration file, *`accesslist_backup.xml`*. The configuration file must exist in the `savedconfig` directory.

4. `restore accesslist mylist1 from accesslist backup.xml` — Restore the access list entries for mylist1 from the saved configuration file, `accesslist_backup.xml`.
5. `show accesslist mylist1` — Display the entries for the restored access list, mylist1. The entries are:
   - 10.1.1.30/32
   - 172.16.255.220/32
   - 209.165.200.225/32
   - chap-username 12h7b.lab2.webservices
   - chap-username 12784.lab1.webservices
   - chap-username test2.sys3
6. `save accesslist mylist1 bootconfig` — If any entries prior to the restore were not saved, issue the `copy` command to save the current access list configuration to the storage router bootable configuration. (Optional)

Restoring AAA Authentication Information

When you restore AAA authentication information, the following configuration settings are updated:

- AAA authentication list
- The user names and passwords in the local username database
- Radius servers and associated server and global authentication port, retransmit, time-out, and key values
- TACACS+ servers, and associated server and global authentication port, time-out, and key values

To restore the AAA authentication configuration that exists in the saved configuration file *aaa_backup.xml*:

1. `enable` — Enter Administrator mode.
2. `show savedconfig aaa_backup.xml` — Display the contents of the backup file and verify that this is the AAA authentication configuration that you want to restore. The file must exist in the `savedconfig` directory.
3. `restore aaa from aaa_backup.xml` — Restore the AAA authentication from the saved configuration file, `aaa_backup.xml`.

4. `show aaa` — Display the AAA authentication information and verify that it is now correct.
5. `save aaa bootconfig` — If you make any changes to the restored AAA authentication configuration, save the changed configuration to the storage router bootable configuration. (Optional)

Restoring VLANs

You can restore specific VLANs or all VLANs. When you restore a VLAN, the VTP mode is also restored.

Use the following procedure to restore a VLAN. In this example, VLAN 10 (named TestLab) will be restored from the saved configuration file named *VLAN_backup.xml*:

Note: In a cluster environment, VLAN configuration must be performed on the first storage router to join the cluster. If you issue a `VLAN` command from another storage router in the cluster, the CLI displays an informational message with the system name and IP address of the storage router that is currently handling all VLAN functions.

---

1. `enable` — Enter Administrator mode.
2. `show savedconfig` *`VLAN_backup.xml`* — Display the contents on the saved configuration file *`VLAN_backup.xml`*. Verify that the file contains the VLAN and VTP configuration information that you want to restore (Example 16).
3. `restore vlan 10 from` *`VLAN_backup.xml`* — Restore VLAN 10 from the saved configuration file *`VLAN_backup.xml`*.
4. `show vlan` — Verify that the VLAN is restored and the configuration is correct.
5. `show vtp` — Verify that the VTP configuration is correct.
6. `save vlan` *`10`* `bootconfig` — If you make any configuration changes to the VLAN after restoration, save the changes to the storage router bootable configuration. (Optional)

Example 16: Show VLAN Information from Saved Configuration File

```
!
! VTP DOMAIN
```

```
!
vtp domain none
!
! VTP MODE
!
vtp mode transparent
!
! VLAN
!
vlan 10 name TestLab mtusize 1500
```

Restoring System Configuration

You can restore selected system information using the `restore system` command. You can restore the following information:

- Administrator contact settings
- SNMP network management configuration
- NTP server and date, time, and time zone settings
- DNS configuration
- IP address of remote syslog host
- Software default download locations and associated user names and passwords
- CDP configuration
- Restrict service setting for all interfaces
- Storage router routing table
- Storage router event message logging table
- Configuration settings for all Fibre Channel interfaces

Use the following procedure to restore system configuration information. In this example, SNMP network management configuration and administrator contact settings will be restored from the saved configuration file named *system_backup.xml*:

1. `enable` — Enter Administrator mode.

2. `show savedconfig` *`system_backup.xml`* — Display the contents of the saved configuration file, *`system_backup.xml`*. Verify that the file contains the SNMP network management configuration and administrator contact information that you want to restore.
3. `restore system snmp from` *`system_backup.xml`* — Restore SNMP network management configuration.
4. `show snmp` — Verify that the SNMP network management information is restored and that the configuration is correct (Example 17).
5. `restore system contactinfo from` *`system_backup.xml`* — Restore administrator contact settings.
6. `show admin` — Verify that the administrator contact information is restored and that the configuration is correct (Example 18).
7. `save system bootconfig` — If you make any configuration changes to the SNMP configuration or administrator contact information after restoration, save the changes to the storage router's bootable configuration. (Optional)

Example 17: Verify SNMP Configuration

```
[SR2122_PR1]# show snmp
First Trap Host: 10.1.32.200
Second Trap Host: 10.2.12.242
Get Community String: public
Set Community String: private
Send Authentication Traps: enabled
Link Up/Down Enable for mgmt: enabled
Link Up/Down Enable for fc1: enabled
Link Up/Down Enable for fc2: enabled
Link Up/Down Enable for fc3: enabled
Link Up/Down Enable for fc4: enabled
Link Up/Down Enable for fc5: enabled
Link Up/Down Enable for fc6: enabled
Link Up/Down Enable for fc7: enabled
Link Up/Down Enable for fc8: enabled
Link Up/Down Enable for ge1: enabled
Link Up/Down Enable for ge2: enabled
```

Example 18: Verify Administrator Contact Information

```
[SR2122_PR1]# show admin
Administrator Contact Information
   Name: Pat Hurley
   Email: phurley@abc123z.com
   Phone: 123.456.7890
   Pager: 123.456.3444 pin 2234
```

Powering Down the Storage Router

If you need to make changes to the physical location or cabling of the storage router, you may need to schedule a time to power down the unit. Use the following procedure to properly power down a storage router. These steps assure that the file system is in the appropriate state prior to shutdown.

1. `enable` — Enter Administrator mode.
2. `halt` — Assure that all configuration information is saved. Respond to any prompts to save information as desired. The storage router can be safely powered down when the `[HALTED]#` command prompt appears.

Resetting the System

There may be times when you need to return some or all of the storage router configurations to factory defaults, for example, when moving a system between environments (such as test and production) or for troubleshooting purposes.

To reset the storage router:

1. Save existing configuration information to a file. (Optional)
2. Clear the current configuration and restore some or all factory defaults, using the `clear conf` command.

Note: If the storage router is operating in a cluster environment, any SCSI routing instances running on this storage router fail over to another storage router in the cluster. If you are operating in a cluster environment but do not want SCSI routing instances to fail over, issue the `no scsirouter enable` command for all instances (or selected instances that should not fail over) before you issue the `clear conf` command. (This will permanently delete the SCSI routing instances from the cluster.) See the "Controlling SCSI Routing Instances in a Cluster" section on page 187 for additional information on operating the storage router in a cluster environment.

3. Run the initial configuration script to configure the management interface via an EIA/TIA-232 console connection. (Optional)
4. Restore specific configuration information or reconfigure the storage router using CLI commands or the web-based GUI.

Reset All to Factory Defaults

If an existing storage router is to be physically moved to another environment, and it is not necessary to retain any current configuration information (system setup will be completely different):

1. `enable` — Enter Administrator mode.
2. `clear conf or clear conf all` *`HP`* — Clear the current system configuration, including network management information.

   For storage routers deployed for SCSI routing, you can use the Clear Conf Wizard. At the prompt, enter the Administrator password. Enter all to erase system configuration and management port settings, and all saved configurations and SCSI routing instances (Example 19). Entering the CLI `clear conf all` command, followed by the Administrator password (for example, hp) will also erase system configuration and management port settings.

   After either of the commands completes, the storage router reboots.

Example 19: Reset storage router Configuration

```
Enter admin password: *****


This process can restore factory default settings for
the SR2122-2.
```

```
* Select "apps" to remove active applications and
retain system
  configuration settings.
* Select "system" to remove active applications and
system
  configuration settings.
* Select "saved" to remove all backup configurations
from disk.
* Select "all" to remove active applications, system
  configuration,   and saved configurations.


The system configuration includes the management port,
dns, admin and monitor login, ntp, and snmp. You will
need to use the console
to reconfigure the management port if you erase the
system configuration.


The system will reboot if you select "apps", "system",
or "all".


Erase what? [apps/system/saved/all/cancel (cancel)]
```

Note: After the move, use the EIA/TIA-232 console connection to configure the management interface IP address and other required system information. (See the "Initial System Configuration Script" section in Chapter 5, "Configuring the Storage Router" for details.) Then configure the storage router via the **Setup Configuration** Wizards or other CLI commands, or via the web-based GUI.

Reset and Retain System Settings

If an existing storage server is going to be used for testing purposes (system configuration information will not be changed) and then restored to its current configuration, use the following procedure:

1. `enable` — Enter Administrator mode.

2. `save all myfile` — Save all configuration information in a file called *myfile*. This file is stored in the `savedconfig` directory.
3. `clear conf` — Clear the current configuration but retain system information (such as management and HA interfaces, logging table, DNS, Administrator and Monitor passwords, NTP server, and SNMP information) and saved configuration files.

   At the prompt, enter the Administrator password. Enter apps to retain system configuration settings.

   The storage router reboots.

   Perform the required user testing. When finished, continue with Step 4 to restore the original configuration.
4. `restore all from myfile` — Restore original configuration, which was retained over the `clear conf` command.
5. `reboot` — Reboot to restore the original application configuration into running memory.

Reset to Remove Saved Configuration Files

Use the following procedure if a standalone storage router has joined a cluster and adopted the new cluster's configuration. The procedure removes previously saved configuration files from the stand-alone period, but the storage router's system configuration, management information, and SCSI routing instances remain unchanged.

1. `enable` — Enter Administrator mode.
2. `clear conf` — Remove all saved configuration files from the `savedconfig` directory.
3. At the prompt, enter the Administrator password. Enter saved to retain system configuration settings.

   All files are removed from the `savedconfig` directory but the storage router does not reboot.
4. `show savedconfig` — Verify that all files have been removed from the `savedconfig` directory.

Note: You can also use the `delete savedconfig` command to delete selected saved configuration files from the `savedconfig` directory.

Recovering Passwords

The storage router management interface is password protected. You must enter passwords when accessing the storage router via Telnet (for the CLI) or the web-based GUI. Password protection can also be enabled for the storage router console interface, requiring that the same Administrator and Monitor mode passwords that are configured for the management interface be applied to the console interface.

If the passwords have been enabled for the console interface and are lost, you can recover management access to the storage router using the password recovery procedure. The password recovery procedure requires physical access to the storage router console and can be found at the following URL:

http://www.hp.com

Controlling SCSI Routing Instances in a Cluster

It is important to know where SCSI routing instances are running. While automatic failover capabilities keep the storage router cluster operational in times of system difficulties, manual HA controls provide the ability to distribute SCSI routing instances between the storage routers in a cluster to meet your specific network requirements.

The following are typical activities involved with controlling SCSI routing instances in a cluster environment. While most of these activities are performed infrequently, some (such as viewing operational statistics) may be performed on a regular basis.

- Making Changes to Instance Configurations
- Enabling and Disabling Connections
- Stopping and Starting Instances
- Viewing Operational Statistics
- Handling Failover

Making Changes to Instance Configurations

Note: To assure that changes are correctly propagated to all storage routers within a cluster, always modify the configuration of a SCSI routing instance from the storage router where the instance is currently active.

Frequently you will make changes to the SCSI routing instance configurations. Changes include such actions as adding or deleting a target, adding or deleting a LUN, remapping a target, or modifying access. It is important to understand the ramifications of these changes on the IP hosts accessing the associated storage resources. For example, changing the instance configuration may change the device presentation to the IP host, effectively changing the name or number assigned to the device by the host operating system. Certain instance configuration changes, such as adding or deleting targets, adding or deleting LUNs within a particular target, or adding or deleting entire instances may change the order of the devices presented to the host. Even if the host is only associated with one SCSI routing instance, the device order could make a difference.

Typically, the IP host operating system assigns drive identifications in the order they are received based on certain criteria. For example, a Linux system assigns drive identifications in the order they are received based on host, bus, target, and LUN information. Changing the order of the storage discovery may result in a changed drive identification. Applications running on the host may require modification to appropriately access the current drives.

If an entire SCSI routing instance is removed, or there are no targets available for the host, the host's iSCSI driver configuration file must be updated to remove the appropriate reference before restarting the iSCSI driver. If a host's iSCSI configuration file contains a reference to an instance which does not exist or has no targets available for the host, the iSCSI driver will not complete a login and will not discover targets associated with any SCSI routing instance.

Enabling and Disabling Connections

A SCSI routing instance becomes active, by default, once it is associated with a Gigabit Ethernet interface to IP hosts. Each target that is added to an instance is also, by default, enabled. However, no IP hosts can connect or log in to that target because the target has no access list association. Once you associate an access list with a target, it is automatically enabled; the IP hosts specified by access list entries are allowed to connect or log in to the target.

Use the `scsirouter target disabled` command to control access to the target without changing the access list association or stopping the entire SCSI routing instance. Existing connections and logins are not affected, but future connections and logins are prohibited.

Use the `scsirouter target enabled` command when you are ready to allow connections and logins again.

For example, suppose you have a problem with an entry in the access list, webserver2. This access list is associated with the target, webstorage2, which is, in turn, associated with the SCSI routing instance foo.

To temporarily disable access to the target associated with a problem access list:

1. `enable` — Enter Administrator mode.
2. `show scsirouter` *`foo`* `stats` — Display status to confirm the SCSI routing instance, foo, is active on this storage router.
3. `show scsirouter` *`foo`* — Verify the name and current status of the target and access list. The target, webstorage2, should be associated with the webserver2 access list and the target should be enabled. (Example 20.)
4. `scsirouter` *`foo`* `target` *`webstorage2`* `disabled` — Disable access to the target, webstorage2. (Example 21)

Example 20: Verify Target, Access List, and Target Status

```
[SR2122-2_PR1]# show scsirouter foo
foo description "test SCSI routing instance"
foo authenticate "none"
foo primary "none"
foo proxy server disabled
foo failover primary "none"
foo failover secondary "none"
foo lun reset no
foo cdb retry counter 30
```

```
foo serverif ge2 10.1.0.45/24, TCP port:3260
foo target webstorage2 description “Web Storage”
foo target webstorage2 Name
“ign.1987-05.com.hp.00.0b1aaa415.....webstorage2”
foo target webstorage2 enabled "TRUE"
foo target webstorage2 accesslist "webserver2"
foo target webstorage2 wwpn "21:00:00:05:ae:42:2f:12"
```

Example 21: Verify New Target Status

```
[SR2122-2_PR1]# show scsirouter foo
foo description “test SCSI routing instance”
foo authenticate “none”
foo primary "none"
foo proxy server disabled
foo failover primary “none”
foo failover secondary “none”
foo lun reset no
foo cdb retry counter 30
foo serverif ge2 10.1.0.45/24,TCP port:3260
foo target webstorage2 description “Web Storage”
foo target webstorage2 Name
“ign.1987-05.com.hp.00.0b1aaa415.....webstorage2”
foo target webstorage2 enabled "FALSE"
foo target webstorage2 accesslist "webserver2"
foo target webstorage2 wwpn "21:00:00:05:ae:42:2f:12"
```

Stopping and Starting Instances

If the storage router is experiencing a problem with a specific set of IP hosts or storage resources, you may wish to stop the associated SCSI routing instance from running anywhere in the cluster. The `no scsirouter enable` command causes the specified SCSI routing instance to cease running on the storage router, but does not cause a failover to another storage router in the cluster. This command effectively stops an instance from running anywhere in the cluster.

Once a SCSI routing instance has been stopped, it can be re-activated by issuing the `scsirouter enable` command. The `scsirouter enable` command must be issued from the same storage router as the `no scsirouter enable` command.

See the *IP Storage Router 2122-2 Command Line Interface User Guide* for command details.

Viewing Operational Statistics

Use the `show scsirouter stats` command to display the status of the SCSI routing instance and to see the number of active connections and the number of logins that have occurred since the storage router was last restarted (or since statistics were last cleared).

For example, the `show scsirouter stats` command in Example 22 shows that SCSI routing instance, **foo**, is currently active.

Example 22: Results of "show scsirouter stats" Command

```
[SR2122-2_PR1]# show scsirouter foo stats


router status    started           iSCSI ver (Min/Max)
logins active
foo    ACTIVE    Jan 11 23:06:08         2/2
          10     7
```

Handling Failover

In a cluster, storage routers continually exchange information as heartbeats to detect failures in the cluster. HA messages are sent using UDP over IP and, depending on the message type or situation, may be sent as unicast or multicast messages. To make sure that HA information is exchanged reliably between storage routers, the storage routers alternate transmission of heartbeats between the management and the HA interfaces.

Failover of SCSI routing instances is automatic when the storage router detects that another storage router in the cluster is no longer responding to heartbeats. Failover of a SCSI routing instance also occurs if the associated Gigabit Ethernet interface is unavailable or if all targets are unavailable.

Note: If some targets are available but others are not, failover of the SCSI routing instance does not occur.

Each cluster supports up to 12 active SCSI routing instances. Since each storage router can also support up to 12 SCSI routing instances, high availability is ensured for each instance in the cluster (regardless of the division of those instances between storage routers).

Manual Failover

While failover of SCSI routing instances is automatic, there may be times when you wish to manually move a SCSI routing instance from one storage router to another. The move may be temporary, after which the instance will be moved back to its original location. At other times, you may want to move a SCSI routing instance permanently to another storage router, ensuring that the instance will continue running on the specified storage router whenever possible.

As an example cluster scenario, a cluster is composed of two storage routers, StorageRouterSys1 and StorageRouterSys2. StorageRouterSys1 is currently running instances, scsi1 and scsi2, and is the primary storage router for both instances. StorageRouterSys2 is currently running instances, scsi3 and scsi4. The primary attribute for scsi3 and scsi4 is set to the default setting of none, indicating no preferred storage router for failover for either instance.

Failover as Temporary Move

Referring to the example cluster scenario just described, the following procedure moves the SCSI routing instance, scsi1, from its primary, or preferred, storage router, StorageRouterSys1, to the other storage router on a temporary basis. The commands in this procedure are issued from a CLI session from storage router, StorageRouterSys1.

1. `enable` — Enter Administrator mode.
2. `show cluster or show scsirouter` *`scsi1`* `stats` — Verify that the instance to be moved, scsi1, is indeed running on storage router, StorageRouterSys1.
3. `failover scsirouter` *`scsi1`* — Failover SCSI routing instance, scsi1.

Note: Because there are only two storage routers in the cluster, you do not need to specify the failover destination.

4. `show cluster or show scsirouter` *`scsi1`* `stats` — Verify that the specified SCSI routing instance, scsi1, is no longer running on the storage router, StorageRouterSys1.

Once the failover is complete, establish a Telnet session to StorageRouterSys2 and verify — using CLI commands described in Step 1 and Step 2 above — that the SCSI routing instance, scsi1, is now running on that storage router.

This is considered a temporary move because StorageRouterSys1 is still designated as the primary storage router for the SCSI routing instance, scsi1. If, for example, StorageRouterSys1 is rebooted, scsi1 will stop running on StorageRouterSys2 and will start up and run on StorageRouterSys1.

Note: Use caution if you change the configuration of a SCSI routing instance while it is running on the storage router that is not the instance's configured primary storage router. If the instance's configuration changes while the designated primary storage router for that instance is down (or otherwise removed from the cluster), the changes will not be propagated to that storage router. When the primary storage router reboots (or otherwise returns to the cluster), it will reassert itself as the primary and will start to run the instance using the last configuration it had before leaving the cluster.

Failover as Permanent Move

Referring to the example cluster scenario previously described, the following procedure moves the SCSI routing instance, scsi2, from its primary, or preferred, storage router, StorageRouterSys1, to the other storage router on a permanent basis. The commands in this procedure are issued from a CLI session from storage router, StorageRouterSys1.

1. `enable` — Enter Administrator mode.
2. `show cluster or show scsirouter` *`scsi2`* `stats` — Verify that the instance to be moved, scsi2, is indeed running on storage router, StorageRouterSys1.
3. `scsirouter` *`scsi2`* `primary` *`StorageRouterSys2`* — Set StorageRouterSys2 as the primary storage router for the desired SCSI routing instance, scsi2.

4. `save scsirouter scsi2 bootconfig` — Save the current SCSI routing instance configuration, including the primary setting, and circulate the changed configuration around the cluster.
5. `failover scsirouter scsi2` — Failover the desired SCSI routing instance, scsi2.

Once the failover is complete, establish a Telnet session to StorageRouterSys2 and verify — using the `show scsirouter scsi2` command — that the SCSI routing instance, **`scsi2`**, is now running on StorageRouterSys2 and that StorageRouterSys2 is designated as the primary storage router for that instance.

Failover for Distribution Purposes

In the example cluster scenario previously described, there is a significant increase in traffic for SCSI routing instance, scsi4, and as a result, you decide to distribute all of the other instances (scsi1, scsi2, and scsi3) to the StorageRouterSys1 storage router. StorageRouterSys1 is already running scsi1 and scsi2.

The following procedure moves the SCSI routing instance, scsi3, to StorageRouterSys1. The commands in this procedure are issued from a CLI session from storage router, StorageRouterSys2:

1. `enable` — Enter Administrator mode.
2. `show cluster` or `show scsirouter scsi3 stats` — Verify that the SCSI routing instance to be moved is indeed running on storage router, StorageRouterSys2.
3. `failover scsirouter scsi3 to StorageRouterSys1` — Failover the desired SCSI routing instance, scsi3, to StorageRouterSys1.

Once the failover is complete, establish a Telnet session to StorageRouterSys1 and verify — using the `show scsirouter` command — that instances, scsi1, scsi2, and scsi3, are now running there.

Note: Because scsi3 has no primary setting, it will remain running on StorageRouterSys1 until it is explicitly stopped or failed over, or until it automatically fails over because an interface is unavailable or a software or hardware problem occurred.

Managing CDP on the storage router

Cisco Discovery Protocol (CDP) is primarily used to obtain protocol addresses of neighboring devices and to discover the platform of those devices. CDP is media- and protocol-independent and runs on all Cisco-manufactured equipment including routers, bridges, access servers, and switches.

Each device configured for CDP sends periodic messages, known as advertisements, to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime, information, which indicates the length of time a receiving device should hold CDP information before discarding it. Each device also listens to the periodic CDP messages sent by others in order to learn about neighboring devices and determine when their interfaces to the media go up or down.

The storage router is enabled, by default, to exchange CDP information with other CDP-enabled devices in the network. CDP can be enable or disabled for individual interfaces on the storage router, and the holdtime for receiving devices and the frequency of CDP transmissions from the storage router can be modified.

Disable CDP for Selected Interfaces

CDP can be enabled or disabled for the management, HA, and Gigabit Ethernet interfaces on the storage router. By default, all interfaces are enabled for CDP. To disable CDP for an interface:

1. `enable` — Enter Administrator mode.
2. `no cdp interface` *`ge2`* `enable` — Disable CDP on the desired interface ge2.
3. `show cdp interface` — Confirm that CDP is disabled for the interface.
4. `save system bootconfig` — Save the CDP change to the storage router's bootable configuration. (Optional)

Modify the CDP Holdtime and Timeout Values

Holdtime is the amount of time the receiving device should hold a CDP packet from the storage router before discarding it. The CDP holdtime value must be set to a higher number of seconds than the CDP timer value (the time between CDP transmissions from the storage router). For example, the default CDP holdtime value is 180 seconds. The default CDP timer value is 60 seconds.

To change the CDP holdtime value and the CDP timer value:

1. `enable` — Enter Administrator mode.
2. `show cdp` — Verify the current CDP configuration.
3. `cdp holdtime` *`300`* — Set the number of seconds 300 that a receiving device should hold the storage router CDP packet.
4. `cdp timer` *`120`* — Set the number of seconds 120 between transmissions of CDP packets from the storage router.
5. `show cdp` — Verify the new CDP configuration. (Optional)
6. `save system bootconfig` — Save the CDP changes to the storage router's bootable configuration. (Optional)

Using Scripts to Automate Tasks

If you frequently issue a series of CLI commands, you can save time by entering those commands into a script for execution purposes. Command scripts are stored in the `script` directory and are simply ASCII text files containing CLI commands.

Follow these rules when creating a command script:

- Commands can start anywhere on a line. The first word on any line that is not preceded by a comment character is considered to be the start of a command string.
- Comments can be added by placing an exclamation point (`!`) or number sign (`#`) character at the beginning of the line or as the first character at any position in the line. Comments are useful for documenting the contents of the file and the expected results. Comments can also be used to prevent a command from executing without removing it from the file by inserting a comment character before the command string.

- You can extend commands across line boundaries by ending a line with a backslash (\ ) as the continuation character (Example 23). Use the continuation character to make long commands more readable. The line sequence is continued until a command line without a continuation character is encountered. If a comment line is used to end a line continuation sequence, you must add a blank line after the comment.

Example 23: Extended Commands:

```
radius-server host 10.5.0.53 \
auth-port 1644 \
timeout 60 \
retransmit 5
! Configure 1st RADIUS server

radius-server host 10.6.0.61
. . .
```

- Scripts can be invoked from other scripts.

When scripts run, the commands and any responses are echoed on the storage router console.

Scripts can be created on any system using any text editor and placed in the `script` directory (`/ata3/script`) of the target storage router using FTP. See the "Using FTP with the Storage Router" section on page 201 for details. You can also use the `copy` command to copy the script file to the storage router using HTTP or TFTP.

Running Command Scripts

Use the following procedure to execute the CLI commands stored in a script file. In this example, the script file is named *`CreateSc`* and must exist in the `script` directory.

1. `enable` — Enter Administrator mode.
2. `show script` *`CreateSc`* — Verify that the script, CreateSc, exists in the `script` directory and that it contains the configuration that you want to recreate.
3. `read script` *`CreateSc`* `or read script` *`CreateSc force`* — Read and execute the CLI commands in the script file. When prompted, confirm that you want to continue and execute the script commands.

Use the **force** keyword to execute the script immediately without asking for confirmation. (Optional)

After the script completes, issue the appropriate `show` commands to verify that the script executed as expected.

Managing the Log File

The storage router can log event information to a series of log files, based on the routing rules specified in the storage router logging table. The default configuration routes all storage router event messages at notification level info or lower to the log file. Use the `show logging` commands to display log file entries and to search for entries that match specific text strings or regular expressions.

Log files are created in the storage router `log` directory (`/ata4/log`). They can occupy up to 4 MB of memory. Once this limit has been reached, the oldest file is removed and a new one is created. The `show logging size` command can be used to display the size of the existing log files. The `show system` command can be used to display the amount of space allocated to log files, and the amount of log file space currently available.

The name of the log file is *messages*, followed by a number (for example, *messages3* or *messages12*). The first log file is named *messages0*, the next log file is named *messages1*, and so on.

Depending on the needs of your enterprise, you can archive log files to a remote server, or you can clear log files on a periodic basis. You can use FTP to transfer files from the storage router to a remote server (see the "Using FTP with the Storage Router" section on page 201 for details), or you can use the web-based GUI to display the contents of the log file and use cut-and-paste techniques to save the information to a local file. You can also issue the `show logging all` command and redirect the output of your console using the logging facilities for your specific console interface.

Note: See the "Understanding Logging" section on page 204 for more information about adding routing rules to the storage router logging table.

Clearing the Log Files

To periodically clear the storage router log files.

1. `enable` — Enter Administrator mode.
2. `show logging size` — Check the current size of the storage router log files (Example 24).
3. `show logging all or show logging last` *`50`* — Display all the current log file entries (first command), or display a selected number of entries, such as 50, from the end of the file (second command).
4. `clear log` — Clear the existing log file. The storage router clears the existing log file and starts a new log file.

Example 24: Results of "show logging size" Command

```
[SR2122-2_PRA]# show logging size
5120 messages (342797 bytes) logged
```

Gathering Troubleshooting Information

If you experience problems with the storage router, you may need to obtain troubleshooting information for HP technical support personnel. The storage router provides several features that can help you assemble the necessary information.

The following are typical activities involved with troubleshooting the storage router:

- Using the Crash Log
- Using FTP with the Storage Router
- Understanding Diagnostics
- Capturing System Messages at Bootup
- Understanding Logging
- Capturing the Storage Router Configuration
- Using Debug Facilities

Using the Crash Log

If the storage router experiences an unexpected problem that forces it to automatically reboot, a special log file is generated. The file is named *crash.txt* and is stored in the `log` directory (`/ata4/log`). You can display the contents of this file to the console using the `show crash` command.

To save the `show crash` command output, redirect the output of your console using the logging facilities for your specific console interface. Depending on your console interface and scroll buffer size, you may also be able to copy and paste the contents from your console into an ASCII text file.

The crash log provides the following information:

- Exception information
- Boot information, including the kernel version and creation date
- Software information
- A list of all tasks, including entry point, task ID and priority for each task
- Task registers and stack trace for each task in the task list
- Net job ring
- A list of all modules, including module ID, data start addresses, and so on.
- A list of all devices and associated drivers
- A list of all drivers, including the number of create, delete, open, close, read, write, and I/O control actions performed
- A list of free memory addresses and a summary of memory usage information
- A list of open file descriptors
- Network interface information, including flags, interface type, addresses, and MTU information for all storage router interfaces
- The storage router route table
- The ARP table
- The storage router host table
- Active Internet connection information, including PCB, connection type (TCP or UDP), receive and send queues, local and foreign addresses, and state for each connection
- Routing statistics
- IP statistics

- ICMP statistics
- TCP statistics
- UDP statistics
- Network stack data pool (MBufs) and cluster pool table information
- NFS authorization
- Mounted NFS file system information
- IDE disk or Flash information, including device types and parameters
- Registered crash dump functions
- Sample registered dump functions
- CPC710 registers at time of exception

Information used to create the *crash.txt* file is periodically written to the *tmpcrash.txt* file in the `log` directory. If a crash occurred at the current time, use the `show crash current` command to display the information as it would be written to the crash log.

Using FTP with the Storage Router

In certain cases, you may want to copy log files from the storage router to another server in your network for analysis purposes, or you may want to copy configuration or script files to another server prior to making them available to another storage router. The storage router includes an FTP daemon; however, the FTP port (port 21) is, by default, restricted.

To enable FTP and to copy the current message log file from the storage router to another server in the network.

1. `enable` — Enter Administrator mode.
2. `show restrict` — Display interface restrictions. If port 21 on the management interface fei0 is closed, use the command in Step 3 to open it.
3. `no restrict mgmt ftp` — Allow FTP functions on the management interface. (Optional)

Once the function is enabled, open the FTP session to the storage router from the server. You will be prompted for a user name and password. The user name is *`admin`* and the password is the storage router Administrator password. The default Administrator password is `hp`.

Note: The user name and the password are case-sensitive.

The storage router log files and crash trace files are stored in the `/ata4/log` directory. Saved configuration files are stored in the `/ata3/savedconfig` directory. Script files are stored in the `/ata3/script` directory.

To use FTP to retrieve the storage router log file, change to the `/ata4/log` directory using the `FTP cd` command. List the files to determine what log file you want to retrieve. (In our example, the log file is *messages0*.) If necessary, specify the binary flag using the `FTP binary` command. Issue the `FTP get` command to retrieve the log file and to copy it to the specified file on your server. When the process completes, close the FTP connection using the `FTP bye` command.

Example 25 illustrates the FTP session just described. In this example, the storage router management interface IP address is 10.1.11.210.

Example 25: FTP Session

```
Server1> ftp 10.1.11.210
Connected to 10.1.11.210.
220 VxWorks (5.4.1) FTP server ready
Name: admin
331 Password required
Password:********
230 User logged in
ftp> cd /ata4/log
250 Changed directory to "/ata4/log"
ftp> dir
200 Port set okay
150 Opening ASCII mode data connection
size           date       time       name
--------       ------     ------     --------
     512    Apr-09-2002  20:46:18   .         <DIR>
     512    Apr-09-2002  20:46:18   ..        <DIR>
   13803    May-16-2002  15:13:56   messages0
   92167    Apr-10-2002  19:14:06   tmpcrash.txt
```

```
226 Transfer complete
ftp: 374 bytes received in 0.02Seconds 23.38Kbytes/sec.
ftp> binary
200 Type set to I, binary mode
ftp> get
(remote-file) messages0
(local-file) SR2122Sys1_Messages
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
40863 bytes received in 0.049 seconds (8.1e+02 Kbytes/s)
ftp> bye
221 Bye...see you later
```

If you had to remove the restriction on the management interface before proceeding with the FTP session, return to the storage router CLI session and re-enable the restriction, using the following procedure.

1. `show restrict` — Verify that port 21 on the management interface is currently open.
2. `restrict mgmt ftp` — Close the management interface to FTP functions. No FTP functions will be allowed.

Understanding Diagnostics

The storage router performs hardware diagnostics when the unit is powered up. Hardware diagnostics cannot be bypassed. If a hardware diagnostic fails, the storage router halts. The boot process cannot be re-initiated.

If you experience a hardware diagnostic failure, contact HP technical support personnel as described in the "HP Technical Support" section in the "About This Guide" Chapter for further instructions.

The storage router performs additional "soft" diagnostics after the hardware diagnostics complete on power up and after every system reboot. If necessary, the soft diagnostics can be bypassed.

If you experience problems with soft diagnostics, contact HP technical support personnel for assistance.

Capturing System Messages at Bootup

The storage router logs a variety of messages to the console during the system boot process. If you are experiencing problems with the storage router, it may be helpful to capture these messages. Use the console interface to perform the boot process and capture the console log using typical external methods.

Understanding Logging

The storage router generates a variety of system event messages. All storage router event and debug messages are issued in the following format:

Example 26: Event Message

```
Mar 18 11:48:05: %SNMP-5-SASAS: SnmpApp starting...
```

```
<timestamp>: %<facility>-<level_number>-<mnemonic>:
<message text>
```

All messages are assigned a notification level, which reflects the priority of the message in the system. Messages with the highest priority are assigned a notification level of emergency. Messages at this level indicate that the system is unusable. Messages with the lowest priority are assigned a notification level of debug. Messages at this level are for troubleshooting purposes. In Example 26, the message level number is 5, indicating a notification level of notice.

Table 17 lists the notification levels, their level number, and their descriptions.

Table 17: Event Message Notification Levels

Notification Level	Level Number	Description
emergency	0	System unusable
alert	1	Immediate action needed
critical	2	Critical conditions
error	3	Error conditions
warning	4	Non-fatal warning conditions
notice	5	Normal but significant conditions
info	6	Informational messages only
debug	7	Information for troubleshooting purposes

Event, trace, and debug messages can be routed to various destinations, based on the notification level of the message and the application area (facility) that generated the message. Table 18 lists the logging destinations and their descriptions. Table 19 lists the logging facilities and their descriptions.

Table 18: Event Message Logging Destinations

Destination	Description
all	Logs the message to all destinations
none	The message is not logged; it is discarded.
console	The message is logged to a serial console CLI session.
logfile	The message is logged to the storage router log file.
rslog	The message is logged to a remote syslog server. Use the logging syslog command to specify the IP address of the remote syslog server.
vty	The message is logged to all Telnet or other virtual terminal CLI sessions.

Table 19: Event Massage Facilities

Facility	Description
AUTH	AAA authentication
CDP	Cisco Discovery Protocol
CONF	Configuration functions
FC	Storage Router Fibre Channel interfaces
GE	Storage Router Gigabit Ethernet interfaces
HA	Storage Router High Availability clusters
IF	Interface manager
INVALID	Generic functions
IPROUTER	Storage Router IP functions
ISCSI	iSCSI functions
MON	Hardware monitor
SNMP	Simple Network Management Protocol
SNMP	Simple Network Management Protocol
SYSLOG	Syslog functions
UI	Storage Router user interface

Messages are routed by creating a list of routing rules that is searched for a facility and notification level match whenever an event or debug message is received. This list of routing rules is known as the storage router logging table.

By default, the logging table includes rules to log all messages at notification level `notice` (or numerically lower levels) to all destinations, and to log all messages at notification level `info` to the storage router log file. Any message that does not find a matching rule is not logged to any destination.

Use the `show logging` command to display the current logging table routing rules and other logging information.

Filtering and Routing Event Messages

The storage router logging table allows messages to be filtered by their facility and notification level and routed to the specified destination(s). When an event message arrives, the logging table rules are searched by facility name and by level until the first match is found. The message is sent to all the destinations specified by the matching rule. If no match is found, the event message is discarded.

When a new routing rule is added, it is appended to the existing table. Use the `logging level` command to add a new routing rule to the logging table; use the `logging #?` command to insert a routing rule into the logging table before the specified entry.

Each facility can have eight notification levels. Each facility and notification level pair can have up to seven destinations.

In Example 27, the facility is SNMP, and the notification level is 5 (notice). If the logging table included the entries in Example14, the event message in Example 27 would match on the first routing rule, and would be sent to all valid destinations. Any message from the SNMP facility at notification level info, and any message from another facility at notification level info (or lower) would match on the second rule and be sent to the storage router console and log file. All messages from any facility at notification level **debug** would be discarded.

Example 27: Example Log Route Entries List

```
Index   Level     Priority  Facility  Route
1       notice    5         SNMP      all
2       info      6         all       console log file
```

The logging table can be saved and retained across the storage router restart. The order of the rules in the logging table is preserved when entries are deleted.

Enabling and Disabling Logging

Logging is enabled by default. By default, the storage router includes the following routing rules in the logging table:

- All messages at notification level notice or lower are logged to all valid destinations.
- All messages at notification level info are logged to the storage router log file.
- All debug messages are discarded.

Use the `no logging on` command to quickly disable logging for all destinations without modifying the storage router logging table. No logging will take place until logging is re-enabled by the `logging on command`.

If you clear the logging table without returning to the factory defaults, all rules are removed from the logging table. This causes all messages to be discarded because there are no matching rules in the logging table. To resume logging, you can add new routing rules, restore a previously saved logging table, or clear the logging table back to the factory defaults.

Viewing and Saving the Log File

You can view the entire storage router log file or selected portions of the log file using the `show logging` command. You can also view the log file using the web-based GUI. If you want to analyze or search the log file in more detail, you can use FTP to retrieve a copy of the log file. See the "Using FTP with the Storage Router" section on page 201 for details.

For additional information about managing the storage router log file, see the "Managing the Log File" section on page 198.

Capturing the Storage Router Configuration

You can use the `show runningconfig` or `show bootconfig` command to display the storage router's current running configuration or bootable configuration. You can then redirect this display to create a script file in the storage router's `script` directory. The resulting file can be used as a basis to create command scripts to automate common tasks. See the "Using Scripts to Automate Tasks" section on page 196 for more details.

Using Debug Facilities

The storage router includes debug facilities for SCSI routing instances. Running debug traces can impact the operation of the storage router. If you experience problems with a SCSI routing instance that cannot be resolved, HP technical support personnel may ask you to capture some debug traces. They will assist you to properly configure the storage router to accomplish this task. By default, debug facilities are disabled for all SCSI routing instances.

Technical Specifications

This appendix gives details about the technical specification of the storage router.

Specifications

This appendix lists the technical specifications in Table 20.

Table 20: Storage Router Specifications

Specifications	
Environmental	
Temperature, ambient operating	50 to 95°F (10 to 35°C)
Temperature, nonoperating and storage	-20 to 140°F (-30 to 60°C)
Humidity (RH), ambient (non-condensing) operating	10 to 70 percent non-condensing
Humidity (RH), ambient (non-condensing) nonoperating and storage	5 to 95 percent non-condensing
Altitude, operating and nonoperating	-500 to 10000 ft (-152.4 to 3048 m)
Physical Characteristics	
Dimensions (H x W x D)	1.75 x 17.44 x 16.13 in. (4.45 x 44.3 x 40.97 cm) 1 RU[1]
Weight	11.25 lb (5.1 kg)
AC power	
Power supply output	70W
System power dissipation	50W
AC current	1.0A maximum @ 100 to 240 VAC
AC frequency	50 to 60 Hz
Airflow	Right side in, left side out
Fuse (F1) rating	3.15A, 250 VAC, time delay, not field-serviceable

1.RU = Rack Unit

Cable and Port Pinouts

This appendix provides cable and port pinout information for the SR2122-2 storage router and includes the following sections:

Gigabit and Fibre Channel Ports

Table 21 lists the types of SFP modules and connectors used with the Gigabit Ethernet and Fibre Channel ports in the storage router. For more information about the SFP modules and connectors, see the standards for the SFP modules and connectors.

Table 21: SFP Modules and Connectors

Port	Compliance	Connector	Medium
Gigabit Ethernet, GE 1 and GE 2	1000 Base-SX	MT-RJ	Fiber-optic
		LC	Fiber-optic
Fibre Channel, FC 1 and FC 2	FC-PI 100/200-M5-SN-I and FC-PI 100/200-M6-SN-I	LC	Fiber-optic

10/100 Ethernet Management and HA Ports

Use modular, RJ-45, straight-through UTP cables to connect the 10/100 Ethernet ports to end systems. Use modular, RJ-45 cross-connect cables to connect to external switches and routers. Figure 52 shows straight-through cables and Figure 53 shows cross-connect cables.

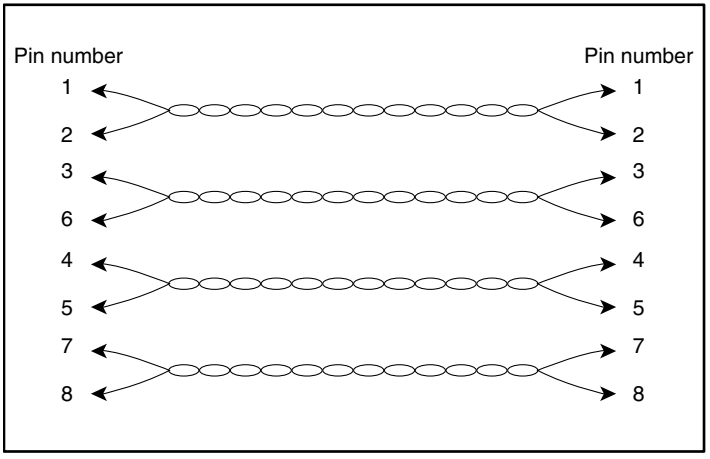


Figure 52: Straight-through cables

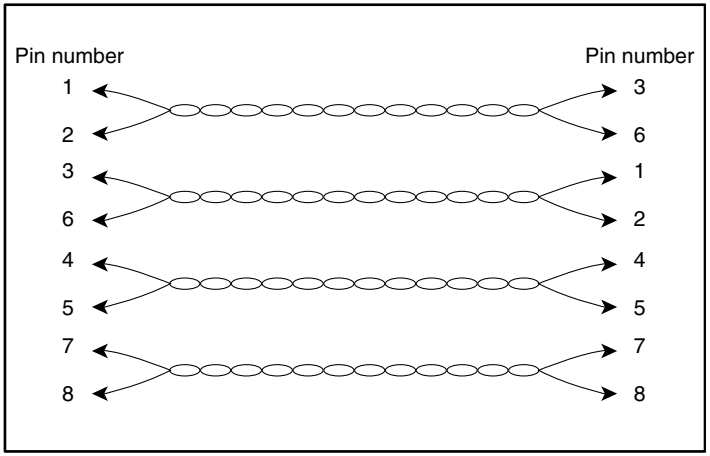


Figure 53: Cross-connect cables

The 10/100 Ethernet ports support RJ-45 connectors. Table 22 lists the signals for RJ-45 connector pinouts.

Table 22: 10/100 Ethernet Management and HA Port Pinouts

Pin	Signal	Direction	Description
1	TD_P	Output	Transmit Data +
2	TD_N	Output	Transmit Data -
3	RD_P	Input	Receive Data +
4			Terminated
5			Terminated
6	RD_N	Input	Receive Data -
7			Terminated
8			Terminated

Console Port

The console port is an EIA/TIA-232 port with a female 8-pin RJ-45 receptacle. Use the rollover cable supplied with the SR2122-2 to connect to the console port. Table 23 lists the console port pinouts.

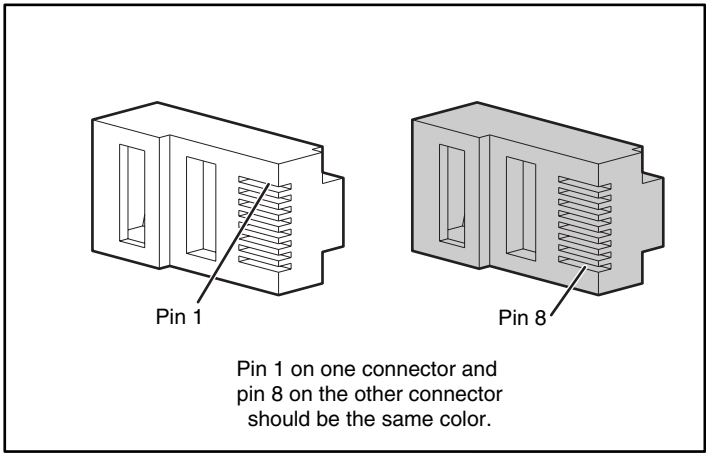


Figure 54: Rollover cable for connection to console port

Table 23: Console Port Pinouts

Pin	Signal	Direction	Description
1	RTS	Output	Request to Send
2	—	—	Not Connected
3	TxD_N	Output	Transmitted Data
4	GND	—	Signal Ground
5	GND	—	Signal Ground
6	RxD_N	Input	Receive Data -
7	—	—	Not Connected
8	CTS	Input	Clear to Send

The console port uses a subset of the EIA/TIA-232 signals. Only the signals TxD_N, RxD_N, CTS and RTS are connected.

Note: The modem control signals are not connected; to access the storage router remotely through the console port, you should do so through a terminal server.

Regulatory Compliance Notices

C

Regulatory Compliance Identification Numbers

For the purpose of regulatory compliance certifications and identification, your product has been assigned a unique HP Series Number. The series number can be found on the product label, along with the required approval markings and information. When requesting compliance information for this product, always refer to this series number. The series number should not be confused with the marketing name or model number of the product.

Federal Communications Commission Notice

Part 15 of the Federal Communications Commission (FCC) Rules and Regulations has established Radio Frequency (RF) emission limits to provide an interference-free radio frequency spectrum. Many electronic devices, including computers, generate RF energy incidental to their intended function and are, therefore, covered by these rules. These rules place computers and related peripheral devices into two classes, A and B, depending upon their intended installation. Class A devices are those that may reasonably be expected to be installed in a business or commercial environment. Class B devices are those that may reasonably be expected to be installed in a residential environment (for example, personal computers). The FCC requires devices in both classes to bear a label indicating the interference potential of the device as well as additional operating instructions for the user.

The rating label on the device shows the classification (A or B) of the equipment. Class B devices have an FCC logo or FCC ID on the label. Class A devices do not have an FCC logo or FCC ID on the label. After the Class of the device is determined, refer to the corresponding statement in the following sections.

Class A Equipment

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at personal expense.

Class B Equipment

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit that is different from that to which the receiver is connected.
- Consult the dealer or an experienced radio or television technician for help.

Declaration of Conformity for Products Marked with the FCC Logo, United States Only

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For questions regarding your product, contact us by mail or telephone:

- Hewlett-Packard Computer Corporation
  P. O. Box 692000, Mail Stop 530113
  Houston, Texas 77269-2000
- 1-800-652-6672 (For continuous quality improvement, calls may be recorded or monitored.)

For questions regarding this FCC declaration, contact us by mail or telephone:

- Hewlett-Packard Computer Corporation
  P. O. Box 692000, Mail Stop 510101
  Houston, Texas 77269-2000
- 1-281-514-3333

To identify this product, refer to the part, series, or model number found on the product.

Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Hewlett-Packard Computer Corporation may void the user's authority to operate the equipment.

Cables

Connections to this device must be made with shielded cables with metallic RFI/EMI connector hoods in order to maintain compliance with FCC Rules and Regulations.

Power Cords

The power cord set included in your server meets the requirements for use in the country where you purchased your server. If you need to use this server in another country, you should purchase a power cord that is approved for use in that country.

The power cord must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cord should be greater than the voltage and current rating marked on the product. In addition, the cross sectional area of the wire must be a minimum of 1.00 mm² or 18AWG, and the length of the cord must be between 6 feet (1.8 m) and 12 feet (3.6 m). If you have questions about the type of power cord to use, contact your HP authorized service provider.

A power cord should be routed so that it is not likely to be walked on or pinched by items placed upon it or against it. Particular attention should be paid to the plug, electrical outlet, and the point where the cord exits from the product.

Mouse Compliance Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Canadian Notice (Avis Canadien)

Class A Equipment

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Class B Equipment

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

European Union Notice

Products with the CE Marking comply with both the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community.

Compliance with these directives implies conformity to the following European Norms (the equivalent international standards are in parenthesis):

- EN55022 (CISPR 22) – Electromagnetic Interference
- EN55024 (IEC61000-4-2, 3, 4, 5, 6, 8, 11) – Electromagnetic Immunity
- EN61000-3-2 (IEC61000-3-2) – Power Line Harmonics
- EN61000-3-3 (IEC61000-3-3) – Power Line Flicker
- EN60950 (IEC950) – Product Safety

Japanese Notice

ご使用になっている装置にVCCIマークが付いていましたら、次の説明文をお読み下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

VCCIマークが付いていない場合には、次の点にご注意下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です　この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

BSMI Notice

警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Laser Device

All HP systems equipped with a laser device comply with safety standards, including International Electrotechnical Commission (IEC) 825. With specific regard to the laser, the equipment complies with laser product performance standards set by government agencies as a Class 1 laser product. The product does not emit hazardous light; the beam is totally enclosed during all modes of customer operation and maintenance.

Laser Safety Warnings

WARNING: To reduce the risk of exposure to hazardous radiation:

- Do not try to open the laser device enclosure. There are no user-serviceable components inside.
- Do not operate controls, make adjustments, or perform procedures to the laser device other than those specified herein.
- Allow only HP authorized service technicians to repair the laser device.

Compliance with CDRH Regulations

The Center for Devices and Radiological Health (CDRH) of the U.S. Food and Drug Administration implemented regulations for laser products on August 2, 1976. These regulations apply to laser products manufactured from August 1, 1976. Compliance is mandatory for products marketed in the United States.

Compliance with International Regulations

All HP systems equipped with laser devices comply with appropriate safety standards including IEC 825.

Laser Product Label

The following label or equivalent is located on the surface of the HP supplied laser device.

This label indicates that the product is classified as a CLASS 1 LASER PRODUCT. This label appears on a laser device installed in your product.

Laser Information

Table 24: Laser Information

Feature	Description
Laser type	Semiconductor GaAlAs
Wave length	780 nm +/- 35 nm
Divergence angle	53.5 degrees +/- 0.5 degrees
Output power	Less than 0.2 mW or 10,869 W m-2 sr-1
Polarization	Circular 0.25
Numerical aperture	0.45 inches +/- 0.04 inches

Electrostatic Discharge

To avoid damaging the system, be aware of the precautions you need to follow when setting up the system or handling parts. A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the device.

To prevent electrostatic damage, observe the following precautions:

- Avoid hand contact by transporting and storing products in static-safe containers.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.
- Place parts on a grounded surface before removing them from their containers.
- Avoid touching pins, leads, or circuitry.
- Always be properly grounded when touching a static-sensitive component or assembly.

Grounding Methods

There are several methods for grounding. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded workstation or computer chassis. Wrist straps are flexible straps with a minimum of 1 megohm ± 10 percent resistance in the ground cords. To provide proper ground, wear the strap snug against the skin.
- Use heel straps, toe straps, or boot straps at standing workstations. Wear the straps on both feet when standing on conductive floors or dissipating floor mats.
- Use conductive field service tools.
- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, have a HP authorized reseller install the part.

Note: For more information on static electricity, or assistance with product installation, contact your HP authorized reseller.

Recommended Host/Storage Configurations

This appendix provides a brief overview of recommended host/storage configuration using the HP SR2122-2 IP Storage Router. Three configurations are discussed:

FCIP Only

Two SAN islands may be joined into a single large, geographically dispersed SAN using the HP SR2122-2s as Fibre Channel to IP gateways to translate between Fibre Channel protocol and FCIP protocol. FCIP protocol transmitted over a WAN network is used to extend the connection between the two SAN islands beyond the nominal 10 km maximum length for direct Fibre Channel.

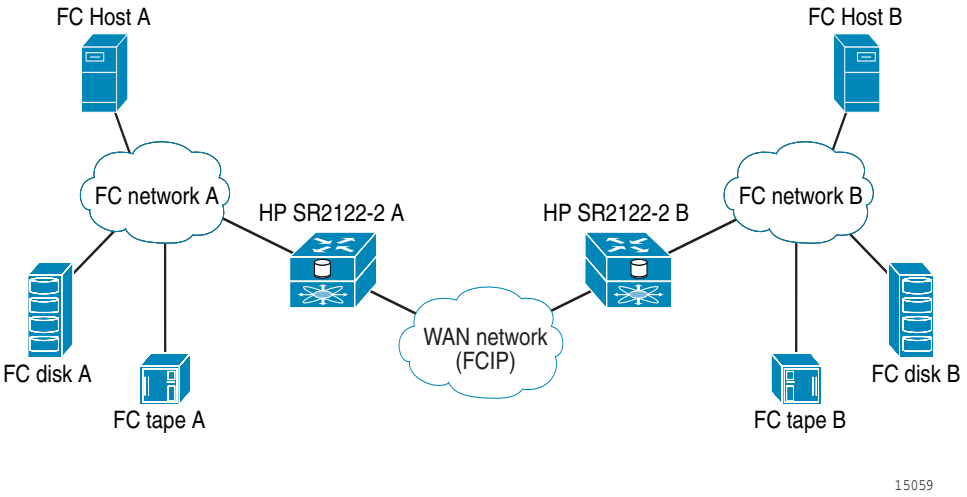


Figure 55: FCIP only

Disk LUNs at either site A or site B may be assigned either to local hosts or to remote hosts.

This basic configuration may also be used when Data Replication Manager or Continuous Access is employed to replicate disk data between the two sites. Since these data replication products use redundant Fibre Channel fabrics, two separate long distance links must be implemented. Although the two Fibre Channel fabrics could be routed through only two SR2122-2s, to avoid a single point of failure, a total of four SR2122-2 units should be included in this configuration.

As shown in Figure 55, a single Fibre Channel connection is required between the SR2122-2 and the Fibre Channel network at each site. The second Fibre Channel port on the SR2122-2 is not used.

The iSCSI protocol is not used in this configuration.

FCIP with Local iSCSI Hosts

One or more host servers may be connected to the extended SAN through a local IP network at site A using the iSCSI protocol. This connection is shown in Figure 56 using the second Gigabit Ethernet port on the site A SR2122-2.

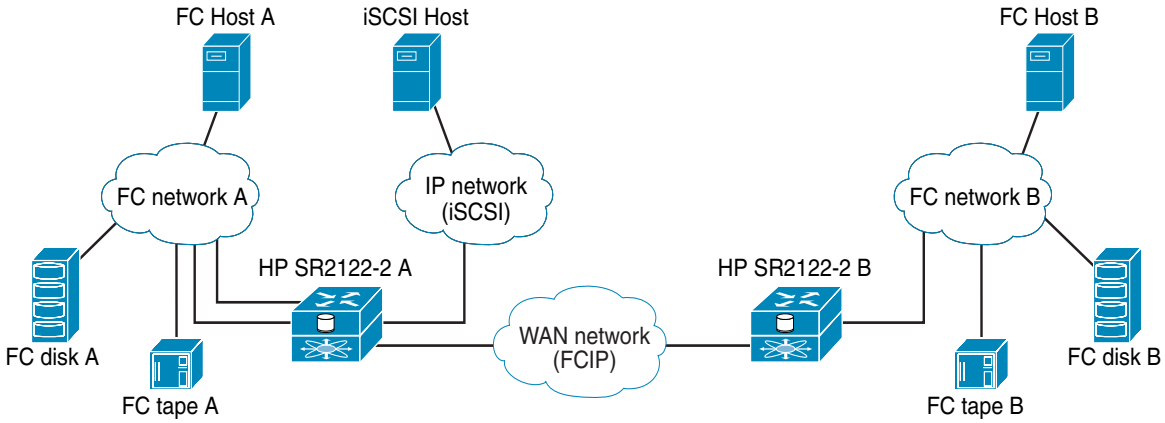


Figure 56: FCIP with local iSCSI hosts

For this configuration, shown in Figure 56, two connections from the SR2122-2 to the Fibre Channel network at site A are required. One SR2122-2 Gigabit Ethernet (Fibre Channel) port is assigned to the FCIP connection and the second is designated for the iSCSI connection.

Disk LUNs at site A may be assigned to the iSCSI hosts. The SR2122-2 translates the iSCSI I/O commands into Fibre Channel protocol commands.

The iSCSI hosts at site A are also able to access the disk LUNs at site B. The iSCSI protocol I/O commands are converted to FCIP protocol in the site A SR2122-2 and transmitted to site B using FCIP. The iSCSI host applications must be able to tolerate the total latency incurred through the multiple protocol conversions plus the overall network delay to access disk LUNs at site B.

A further expansion of this configuration would be to mirror the site A iSCSI configuration to include iSCSI hosts at site B. This would provide access to site B disk LUNs, as well as site A disk LUNs, through the SR2122-2 at site B.

FCIP with Remote iSCSI Hosts

The FCIP configuration with local iSCSI hosts may be extended by locating the iSCSI hosts apart from either site A or site B. This configuration requires that the iSCSI IP network be connect to the large SAN through a WAN network as shown in Figure 57.

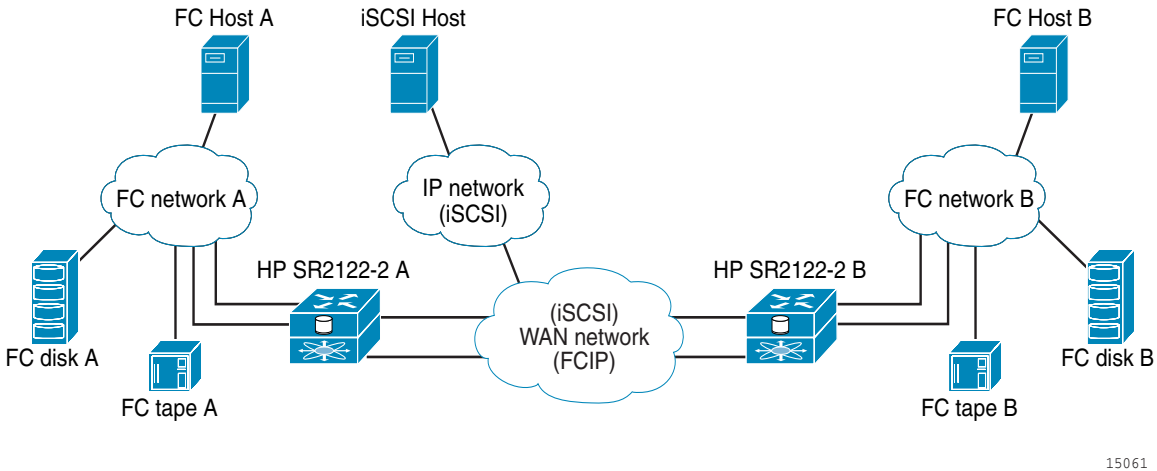


Figure 57: FCIP with remote iSCSI hosts

This configuration allows the iSCSI hosts to access disk LUNs at either site A or site B, providing maximum configuration flexibility.

Note: Within the WAN network the iSCSI protocol traffic is kept isolated from the FCIP protocol traffic and connects to the SR2122-2s through the second Gigabit Ethernet port on each gateway.

The SR2122-2 has the capability to rate-limit or "pace" the FCIP protocol traffic that it handles. This is accomplished using standard Fibre Channel flow control mechanisms which allows the user to limit the amount of FCIP traffic through the SR2122-2 so that it does not exceed the bandwidth allotted for this connection through the WAN network.

However, the iSCSI protocol traffic has no corresponding flow control mechanism. If the iSCSI protocol traffic and the FCIP protocol traffic are combined on a single network and if the combined traffic exceeds the available

network bandwidth, the iSCSI protocol traffic can theoretically consume some or all of the bandwidth allotted to the FCIP connection. If that happens, both iSCSI and FCIP I/O commands are subject to failure due to dropped packets in the WAN network. By isolating the iSCSI protocol from the FCIP protocol using separate network connections, it is possible to prevent a failure in the FCIP portion of the system due to over-subscription of the WAN connection.

Index

C

G

H

I

L

M

N

O

P

R

S

T

U

V

W